A Robust Remote User Authentication Scheme against Smart Card Security Breach

Chun-Ta Li, Cheng-Chi Lee, Chen-Ju Liu, Chin-Wen Lee

A Robust Remote User Authentication Scheme Against Smart Card Security Breach

Chun-Ta Li[1], Cheng-Chi Lee[2,3,*], Chen-Ju Liu[1], and Chin-Wen Lee[1]

[1] Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.)
th0040@mail.tut.edu.tw
[2] Department of Library and Information Science, Fu Jen Catholic University
510 Jhongjheng Road, New Taipei City 24205, TAIWAN (R.O.C.)
[*]Corresponding author:cclee@mail.fju.edu.tw
[3] Department of Photonics and Communication Engineering, Asia University
500 Lioufeng Road, Taichung City 41354, TAIWAN (R.O.C.)

Abstract. Remote user authentication is important to identify whether communicating parties are genuine and trustworthy using the password and the smart card between a login user and a remote server. Recently, we find that Kim et al.'s password-based authentication scheme [1] assume that the attacker cannot extract the secret information of the smart card. However, in reality, the authors in [2, 8] show that the secrets stored in the card can be extracted by monitoring its power consumption. Therefore, Kim et al.'s scheme fail to resist smart card security breach. As the main contribution of this paper, a robust remote user authentication scheme against smart card security breach is presented, while keeping the merits of the well-known smart card based authentication schemes.

Keywords: Cryptanalysis; Network security; Password; Remote user authentication; Smart card.

1 Introduction

With the significant advances in communication networks over the last couple of decades, remote user authentication based on passwords [1, 3, 6, 7] or biometrics [4, 5] over insecure networks is the conventional method of authentication and has already been accepted warmly. Typically a network of remote servers are responsible for managing and supplying network services to login users for which user authentication protocols have been provided during a login procedure.

Recently, Liao et al. [7] proposed nine requirements for rating performance of a new password authentication scheme in terms of security, friendliness and efficiency. A new password authentication scheme using smart cards should satisfy the following requirements: (1) without maintaining verification tables; (2) users can freely choose and update passwords; (3) resistance to password disclosure to the server; (4) prevention of masquerade attacks; (5) resistance to replay, modification, parallel session and stolen-verifier attacks; (6) a easy-to-remember

password; (7) low communication cost and computation complexity; (8) achieve mutual authentication between login users and remote servers; (9) resistance to guessing attacks even if the smart card is lost or stolen by attackers. Besides requirements stated in reference [7], we list three additional requirements to solve all problems in smart card-based authentication schemes, including: (10) session key agreement; (11) resistance to insider attacks; (12) prevention of smart card security breach attacks. For Requirement (12), it is important to note that secret information stored in a smart card can be extracted by analyzing and monitoring its power consumption [2, 8]. Obviously, if a legal user's smart card is lost and it is picked up by a malicious attacker or an attacker steals user's smart card, the user's sensitive password may be derived out by an attacker. After that, there is no way to prevent the attacker from masquerading as the legal user. In this paper, we focus on the security of password authentication schemes for the merit that the design scheme achieves Requirement (12) and we will propose a robust remote user authentication scheme with better security strength while keeping the above-mentioned requirements.

The remainder of the paper is organized as follows. Section 2 is a brief review of Kim et al.'s authentication scheme and we show their security weaknesses in Section 3. The new remote user authentication scheme against smart card security breach is proposed in Section 4. Security analysis of the proposed scheme is presented in Section 5 and Section 6 concludes the paper.

2 A Review of Kim et al.'s scheme

In this section, we review Kim et al.'s password-based remote authentication scheme [1] and their scheme is composed of three phases, registration, authentication and password update. For convenience of description, terminology and notations used in the paper are summarized as follows:

- U_i: The login user.
- (ID_i, PW_i, SC_i): The identity, password and the smart card of U_i.
- S: The remote server.
- X: The master secret key, which is kept secret and only known by S.
- N: The number of times U_i re-registers to S.
- SK: The common session key.
- $\oplus$: The bitwise XOR operation.
- $H(\cdot)$: A collision free one-way hash function.
- $||$: String concatenation.
- $E_K(.)/D_K(.)$: The symmetric encryption/decryption function with key K.
- $\Longrightarrow$: A secure channel.
- $\longrightarrow$: A public channel.

2.1 Registration Phase

(R.1) $U_i \Longrightarrow S : ID_i, PW_i$
U_i choose his/her identity ID_i and password PW_i and submits $\{ID_i, PW_i\}$ to the remote authentication server S.

(R.2) $S \Longrightarrow SC_i : K_1, K_2, R, H(\cdot)$

Upon receiving U_i's login request, S computes $K_1 = H(ID_i \oplus X) \oplus b$, $K_2 = H(ID_i \oplus X \oplus b) \oplus H(PW_i \oplus H(PW_i))$, and $R = K_1 \oplus H(PW_i)$ and stores K_1, K_2, R, and $H(\cdot)$ into the smart card SC_i, where b is a random number unique to the user U_i. Finally, S releases SC_i to U_i and the registration phase is completed.

2.2 Authentication Phase

(A.1) $SC_i \longrightarrow S : ID_i, T_{U_i}, C_1, C_2$

The user U_i enters ID_i and PW_i and the smart card SC_i computes $C_1 = R \oplus H(PW_i)$ and checks if C_1 is equal to the stored K_1. If it does not hold, SC_i terminates U_i's login request; otherwise, it computes $C_1' = K_2 \oplus H(PW_i \oplus H(PW_i))$ and $C_2 = H(C_1' \oplus T_{U_i})$, where T_{U_i} is the current timestamp generated by U_i. Then, SC_i submits $\{ID_i, T_{U_i}, C_1, C_2\}$ to the server.

(A.2) $S \longrightarrow SC_i : T_S, C_3$

Upon receiving the login request, S verifies the validity of T_{U_i}. If it is invalid, S rejects U_i's login request; otherwise, S checks if the hashed value $H(H(ID_i \oplus X \oplus M') \oplus T_{U_i})$ is equal to received C_2, where $M' = C_1 \oplus H(ID_i \oplus X)$. If it does not hold, SC_i terminates communication; otherwise, S succeeds to authenticate U_i and submits T_S and $C_3 = H(H(ID_i \oplus X \oplus M') \oplus C_2 \oplus T_S)$ to SC_i, where T_S is the current timestamp generated by S. Upon receiving the message from S, SC_i verifies the validity of T_S. If it is invalid, U_i terminates communication; otherwise, U_i checks if the hashed value $H(C_1' \oplus C_2 \oplus T_S)$ is equal to received C_3. If it holds, U_i succeeds to authenticate the remote server S.

2.3 Password Update Phase

In this phase, U_i inserts SC_i into the card reader and enters ID_i and PW_i. Then, SC_i computes $K_1' = R \oplus H(PW_i)$ and checks if the value K_1' is equal to stored K_1. If it does not hold, SC_i rejects U_i's password update request; otherwise, U_i enters a new password PW_i' and SC_i computes $R' = K_1' \oplus H(PW_i')$ and $K_2' = K_2 \oplus H(PW_i \oplus H(PW_i)) \oplus H(PW_i' \oplus H(PW_i'))$ and replaces (R, K_2) with (R', K_2').

3 The Various Kinds of Attacks with Smart Card Security Breach

In this section, we show some attacks with smart card security breach in Kim et al.'s authentication scheme. Let us consider the following scenarios. If a user's smart card is lost and it is picked up by an attacker U_A or an attacker steals user's smart card. The secrets stored in the smart card can be extracted by monitoring its power consumption [2, 8], then the attacker can off-line guess user's password and masquerade as a legitimate user.

3.1 Off-line Password Guessing Attack on Kim et al.'s Scheme

In Kim et al.'s scheme [1], the attacker U_A can breach the secrets $K_1 = H(ID_i \oplus X) \oplus b$, $R = K_1 \oplus H(PW_i)$ and $H(\cdot)$, which are stored in the smart card. Then, U_A can use the breached secrets K_1, R and $H(\cdot)$ to perform the following steps:

Step 1. Select a guessed password PW_i^*.
Step 2. Compute $K_1' = R \oplus H(PW_i^*)$.
Step 3. Compare K_1 to K_1'.

A match in Step 3 above indicates the correct guess of user's password. Therefore, the attacker succeeds to guess the low-entropy password PW_i and Kim et al.'s scheme is vulnerable to off-line password guessing attack.

3.2 Masquerading Attack on Kim et al.'s Scheme

Once the attacker U_A has correctly derived the user's password PW_i, he/she can also use the stored information on the stolen or lost smart card to forge a valid login request to masquerade as a legal user.

During the authentication phase of Kim et al.'s scheme, the attacker U_A can use the information on the lost or stolen smart card to make a valid login request with ease. For example, U_A is able to compute $C_1^* = R \oplus H(PW_i^*)$ and $C_2^* = K_2 \oplus H(PW_i^* \oplus H(PW_i^*) \oplus T_{U_A})$ by using the current timestamp T_{U_A} and the derived password PW_i^* on the lost or stolen smart card. Finally, U_A can successful make a valid login request message to impersonate U_i by sending $\{ID_i, T_{U_A}, C_1^*, C_2^*\}$ to the server S.

4 The Proposed Scheme

In this section, we describe a robust remote user authentication scheme which resolves all the above security flaws of smart card security breach. There are four phases in our scheme - registration, login, verification and password update.

4.1 Registration Phase

(R.1) $U_i \Longrightarrow S : ID_i, H(H(PW_i \oplus RN_1))$
To register, the user U_i chooses his/her identity ID_i and password PW_i and generates a random number RN_1. Then, U_i computes $H(H(PW_i \oplus RN_1))$ and sends ID_i and $H(H(PW_i \oplus RN_1))$ over a secure communication channel to S.

(R.2) $S \Longrightarrow SC_i : ID_i, C_1, H(\cdot)$
Upon receiving ID_i and $H(H(PW_i \oplus RN_1))$, S maintains a account table (AT) for a registration service and the format of AT is shown as follows:

User identity	Registration times	Verification parameter
ID_i	$N = 0$	$H(H(PW_i \oplus RN_1))$

where the 1st field of AT records the user's identity, the 2nd field of AT records $N = 0$ if it is U_i's initial registration, otherwise, S sets $N = N + 1$ in the existing field for U_i, and the 3rd field records U_i's verification parameter $H(H(PW_i \oplus RN_1))$ for a later login request.
Finally, S computes $C_1 = H(ID_i||X||N) \oplus H(H(PW_i \oplus RN_1))$ and stores $\{ID_i, C_1, H(\cdot)\}$ into the smart card SC_i and releases it to U_i.

(R.3) $U_i \Longrightarrow SC_i : ID_i, C_1, H(\cdot), RN_1$
Upon receiving SC_i, U_i stores RN_1 into SC_i and U_i finishes the registration procedure. Note that U_i's SC_i contains $\{ID_i, C_1, H(\cdot), RN_1\}$ and U_i does not need to remember RN_1 after finishing this phase. Note that the bit length of random numbers RN_i and S's master secret key X are assumed to be 256. That is, RN_i and X are two high entropy random numbers.

4.2 Login Phase

When U_i wants to login S, the following operations will perform:

(L.1) $U_i \Longrightarrow SC_i : ID_i, PW_i, RN_2$
U_i inserts his/her SC_i into the smart card reader and enters ID_i, PW_i and a new random number RN_2, where RN_2 is used for next login request. Then, SC_i generates a random number RC and computes $C_2 = H(PW_i \oplus RN_1)$, $C_3 = C_1 \oplus H(C_2)$, $C_4 = C_3 \oplus C_2$, and $C_6 = E_{K_{U_i}}(C_5, RC)$, where $C_5 = H(H(PW_i \oplus RN_2))$ and $K_{U_i} = H(C_2||C_3)$.

(L.2) $SC_i \longrightarrow S : ID_i, C_4, C_6$
SC_i sends $\{ID_i, C_4, C_6\}$ over a public communication channel to the remote server S.

4.3 Verification Phase

Upon receiving the login request from U_i, the remote server S and the smart card SC_i performs the following operations:

(V.1) $S \longrightarrow SC_i : E_{K_S}(RC, RS, C_5)$
If ID_i is invalid, S rejects U_i's login request. Otherwise, S computes $C_7 = H(ID_i||X||N)$, $C_8 = C_4 \oplus C_7$, and $C_9 = H(C_8)$ and compares the third entry $H(H(PW_i \oplus RN_1))$ to the computed C_9. If equal, S successfully authenticates U_i and computes symmetric key $K'_{U_i} = H(C_8||C_7)$, which equals to $K_{U_i} = H(C_2||C_3)$, to obtain (C_5, RC) by decrypting $D'_{K_{U_i}}(C_6)$. Then, S replaces the third entry $H(H(PW_i \oplus RN_1))$ with $C_5 = H(H(PW_i \oplus RN_2))$ and sends $E_{K_S}(RC, RS, C_5)$ over a public communication channel to the smart card SC_i, where RS is a random number generated by S and $K_S = H(C_7||C_8)$. Finally, the format of AT is shown as follows:

User identity	Registration times	Verification parameter
ID_i	$N = 0$	$H(H(PW_i \oplus RN_2))$

(V.2) $SC_i \longrightarrow S : H(RS)$

Upon receiving the message from S, SC_i computes symmetric key $K'_S = H(C_3||C_2)$, which equals to $K_S = H(C_7||C_8)$, to obtain (RC, RS, C_5) by decrypting $D'_{K_S}(E_{K_S}(RC, RS, C_5))$. Then, SC_i verifies if generated (RC, C_5) equals received (RC, C_5). If not equivalent, SC_i terminates communication; otherwise, SC_i now successfully authenticates S and replaces original RN_1 and C_1 with new RN_2 and $C_3 \oplus C_5$, respectively. Finally, SC_i sends a response $H(RS)$ to S and S can make sure that it is communicating with a legitimate U_i. Note that both U_i and S can compute the agreed session key $SK = H(RC \oplus RS)$ for securing future communications.

4.4 Password Update Phase

This phase is extremely similar to the login and verification phases of the proposed scheme and U_i is strongly recommended not to use any previous parameters for his/her update request, e.g. random number RN_2. When a user U_i wants to update his/her password PW_i with a new password PW'_i, U_i inserts his/her SC_i into the smart card and enters his/her ID_i, the original password PW_i, the new password PW'_i, and a new random number RN_3. Then, SC_i computes $C_2 = H(PW_i \oplus RN_2)$, $C_3 = C_1 \oplus H(C_2)$, $C_4 = C_3 \oplus C_2$, and $C_6 = E_{K_{U_i}}(C'_5, RC)$, where $C'_5 = H(H(PW'_i \oplus RN_3))$ and $K_{U_i} = H(C_2||C_3)$. Finally, SC_i sends $\{ID_i, C_4, C_6\}$ over a public communication channel to the remote server S. Upon receiving the message, S performs Step (V.1) and finally the format of AT is shown as follows:

User identity	Registration times	Verification parameter
ID_i	$N = 0$	$C'_5 = H(H(PW'_i \oplus RN_3))$

Note that the new password PW'_i and the new random number RN_3 stored in S's AT are simultaneous updated. Moreover, SC_i replaces original RN_2 and C_1 with new RN_3 and $C_3 \oplus C'_5$, respectively. Now, the new password PW'_i and the new random number RN_3 are successfully updated and this phase is terminated.

5 Security Analysis of The Proposed Scheme

The proposed authentication scheme benefits from the protection of smart cards to prevent the secret information for an attacker to steal and guess the real secrets stored in the stolen smart card or in the exchange of authentication messages. In the following propositions, we give an in-depth analysis of the proposed scheme in terms of security properties.

Proposition 1. *The present scheme is secure against off-line password guessing attack with smart card security breach.*

Proof. With the assumption that the attacker can collect the transmitted messages $\{ID_i, C_4 = H(ID_i||X||N) \oplus H(PW_i||RN_i), C_6 = E_{K_{U_i}}(H(H(PW_i \oplus$

$RN_{i+1}))), E_{K_S}(RC, RS, H(H(PW_i \oplus RN_{i+1}))), H(RS)\}$ and extract the secrets $\{ID_i, C_1 = H(ID_i||X||N) \oplus H(H(PW_i \oplus RN_{i+1})), H(\cdot), RN_{i+1}\}$ stored in the lost or stolen smart card, where $i = 1, 2, 3, \ldots$, $K_{U_i} = H(H(PW_i \oplus RN_i)||H(ID_i||X||N))$ and $K_S = H(H(ID_i||X||N)||H(PW_i||RN_i))$.

Throughout the proposed scheme, U_i's password PW_i makes four appearances as $C_4 = H(ID_i||X||N) \oplus H(PW_i||RN_i)$, $C_6 = E_{K_{U_i}}(H(H(PW_i \oplus RN_{i+1})))$, $E_{K_S}(RC, RS, H(H(PW_i \oplus RN_{i+1})))$ and $C_1 = H(ID_i||X||N) \oplus H(H(PW_i \oplus RN_{i+1}))$. However, for each new login request, the previous random number RN_i stored in the smart card have to be replaced with new random number RN_{i+1}. Therefore, an attacker cannot launch off-line password guessing attack without knowing the previous secret RN_i and our proposed authentication scheme can resist off-line password guessing attack with smart card security breach.

Proposition 2. *The proposed scheme can withstand masquerade attack with smart card security breach.*

Proof. Let us assume an attacker U_A has extracted smart card's secrets and has got the transmitted messages between U_i and S. U_A inserts U_i's SC_i into the card reader and then enters the guessing password PW_i^* and a random number RN_i^*. As described above, throughout the proposed scheme, if any trial value of the password is used during an on-line session, U_A has only one chance to guess the original password to pass server's validation. Once U_A's guessing password is wrong, the server can immediately detect the validity of fake login request and terminate U_A's login session. In this case, U_A cannot masquerade as a legal user to send a valid login request message and the masquerade attack cannot work in the proposed scheme.

Proposition 3. *The proposed scheme is able to provide mutual authentication and a agreed session key between U_i and S in every login session.*

Proof. By the proposed scheme, let us assume that A and B be the two communication parties, namely the login user and the remote server. Let $A \overset{SK}{\longleftrightarrow} B$ denotes the agreed session key SK shared between A and B. Hence, the mutual authentication is achieved between A and B if there exists a session key SK, then A would believe $A \overset{SK}{\longleftrightarrow} B$, and B would believe $A \overset{SK}{\longleftrightarrow} B$. As a result, we have stated that a strong mutual authentication should satisfy the following equations:

$$A \quad believes \quad B \quad believes \quad A \overset{SK}{\longleftrightarrow} B. \tag{1}$$

$$B \quad believes \quad A \quad believes \quad A \overset{SK}{\longleftrightarrow} B. \tag{2}$$

In Step (L.2) of the login phase, after B receives the login request $\{A, C_4 = H(A||X||N) \oplus H(PW_A \oplus RN_i), C_6 = E_{K_A}(H(H(PW_A \oplus RN_{i+1})), RC)\}$, B will verify $H(PW_A \oplus RN_i)$ by computing $C_4 \oplus H(A||X||N)$ and check whether the hashed value $H(C_4 \oplus H(A||X||N))$ is equal to $H(H(PW_A \oplus RN_i))$. If it holds, B decrypts C_6 and gets RC in Step (V.1) of the verification phase. Moreover, B

generates RS and submits $E_{K_S}(RC, RS, C_5 = H(H(PW_A \oplus RN_{i+1}))$ to A. After A receives the response message, A will verify $H(H(PW_A \oplus RN_{i+1}))$ and RC by computing $D_{H(H(A||X||N)||H(PW_A \oplus RN_i))}(E_{K_S}(RC, RS, C_5 = H(H(PW_A \oplus RN_{i+1}))))$. If these values are valid, A computes the session key $SK = H(RC \oplus RS)$ and believes $A \overset{SK}{\longleftrightarrow} B$. Since RC is chosen by A, A believes B believes $A \overset{SK}{\longleftrightarrow} B$. Also, in Step (V.2) of the verification phase, a response $H(RS)$ will be sent to B. After B received the response message from A, B uses RS to compute $H(RS)$ and checks whether the hashed value contains a response RS. If it holds, B believes $A \overset{SK}{\longleftrightarrow} B$. Since RS is chosen by B, B believes A believes $A \overset{SK}{\longleftrightarrow} B$. Finally, after Equations (1) and (2) are satisfied, and together they accomplish the mutual authentication and dynamic session key agreement in the proposed scheme.

6 Conclusions

This paper proposed a robust user authentication scheme using smart cards. We have showed that the proposed scheme avoids smart card security breach attacks and maintains the merits of related works such as provision of mutual authentication, prevention of password guessing attack, detection of masquerade attack, session key agreement, and so on. In our future works, a formal security proof and a experimental simulation would have been a better picture to demonstrate the feasibility of the proposed scheme. and the proposed scheme can be further extended with the countermeasure against the Denial-of-Service (DoS) attacks.

References

1. S. K. Kim and M. G. Chung, "More secure remote user authentication scheme," *Computer Communications*, 32(6):1018–1021, 2009.
2. P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in *Proceedings of Advances in Cryptology*, pages 388-397, 1999.
3. L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, 24(11):770–772, 1981.
4. C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, 33(1):1–5, 2010.
5. C. T. Li and 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):2181–2188, 2010.
6. C. T. Li and 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.
7. I. E. Liao, C. C. Lee and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, 72(4):727–740, 2006.
8. T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, 51(5):541–552, 2002.