Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards

Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo

Abstract — *Recently, Ku-Chen proposed an improvement to Chien et al.'s scheme to prevent from some weaknesses. However, the improved scheme is not only still susceptible to parallel session attack, but also insecure for changing the user's password in password change phase. Accordingly, the current paper presents an enhancement to resolve such problems. As a result, the proposed scheme enables users to change their passwords freely and securely without the help of a remote server, while also providing secure mutual authentication*[1].

Index Terms — Authentication, cryptography, password, parallel session attack

I. INTRODUCTION

In 2002, Chien et al. [1] proposed an efficient password based remote user authentication scheme, and claimed that their scheme has the merits of providing mutual authentication, freely choosing password, no verification table, and involving only few hashing operations. Unfortunately, Ku-Chen [2] pointed out that Chien et al.'s scheme is vulnerable to a reflection attack [3] and an insider attack [4]. In addition, they showed that Chien et al.'s scheme is not reparable [5] once a user's permanent secret is compromised. Furthermore, Ku-Chen proposed an improvement to Chien et al.'s scheme to prevent from above mentioned weaknesses. However, the improved scheme is not only still susceptible to parallel session attack proposed by Hsu [6], but also insecure for changing the user's password in password change phase. Accordingly, the current paper presents an enhancement to resolve such problems. As a result, the proposed scheme enables users to change their passwords freely and securely without the help of a remote server, while also providing secure mutual authentication.

II. REVIEW OF KU-CHEN'S SCHEME

The notations used throughout this paper can be summarized as follows:

- U denotes the user.
- ID denotes the identity of U.
- PW denotes the password of U.
- S denotes the remote server.
- x denotes the permanent secret key of S.
- $h()$ represents a cryptographic hash function.
- $\Rightarrow$ represents a secure channel.
- $\rightarrow$ represents a common channel.

There are four phases in Ku-Chen's scheme – registration, login, verification and password change.

Registration: This phase is invoked whenever U initially registers or reregisters to S. Let n denote the number of times U re-registers to S.

1. U selects a random number b and computes $h(b \oplus PW)$.
2. $U \Rightarrow S$: ID, $h(b \oplus PW)$.
3. If it is U's initial registration, S creates an entry for U in the account database and stores $n = 0$ in this entry. Otherwise, S sets $n = n + 1$ in the existing entry for U. Next, S computes
$$R = h(EID \oplus x) \oplus h(b \oplus PW)$$
where $EID = (ID \| n)$.
4. $S \Rightarrow U$: a smart card containing R and $h()$.
5. U enters b into his smart card.

Note that U's smart card contains R, b, and $h()$, and U does not need to remember b after finishing Step 5.

Login: This phase is invoked whenever U wants to login S.

1. U inserts his smart card into the smart card reader of a terminal, and then enters ID and PW.
2. U's smart card performs the following computations:
$$c_1 = R \oplus h(b \oplus PW)$$
$$c_2 = h(c_1 \oplus T_U)$$
where T_U denotes U's current timestamp.
3. $U \rightarrow S$: ID, T_U, c_2.

Verification: This phase is invoked whenever S receives U's login request.

1. If either ID or T_U is invalid, S rejects U's login request. Otherwise, S computes $h(h(EID \oplus x) \oplus T_U)$. If the computed result equals the received c_2, S accepts U's login request and computes $c_3 = h(h(EID \oplus x) \oplus T_S)$, where T_S denotes S's current timestamp. Otherwise, S rejects U's login request.
2. $S \rightarrow U$: T_S, c_3.
3. If either T_S is invalid or $T_S = T_U$, U terminates this session. Otherwise, U computes $h(c_1 \oplus T_S)$ and then compares the result to the received c_3. If equal, U successfully authenticates S.

[1] This work was supported by the Brain Korea 21 Project in 2004.

Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo are with the Department of Computer Engineering, Kyungpook National University, South Korea (e-mail: yook@knu.ac.kr).

Contributed Paper
Manuscript received April 3, 2004

Password Change: This phase is invoked whenever U wants to change his password PW with a new one, say PW_{new}.

1. U inserts his smart card into the smart card reader of a terminal, enters ID and PW, and requests to change password. Next, U enters PW_{new}.
2. U's smart card computes
$$R_{new} = R \oplus h(b \oplus PW) \oplus h(b \oplus PW_{new})$$
which yields $h(EID \oplus x) \oplus h(b \oplus PW_{new})$, and then replaces R with R_{new}.

III. Cryptanalysis of Ku-Chen's Scheme

In this section, we will show that Ku-Chen's scheme is vulnerable to a parallel session attack [6] and insecure for changing the user's password in password change phase.

A. Parallel Session Attack

In the verification phase, consider the scenario of the parallel session attack that an intruder U_a without knowing user's passwords wants to masquerade as a legal user U by creating a valid login message from the eavesdropped communication between S and U. When U wants to login the remote server S, U sends the login message $\{ID, T_U, c_2\}$ to S, where T_U is the current time stamp. If $\{ID, T_U, c_2\}$ is valid, the identification of U is authenticated and S responses $\{T_S, c_3\}$ to U, where T_S is the current time stamp. Once U intercepts this message, he masquerades as the legal user U to start a new session with S by sending $\{ID, T_U^*, c_2^*\}$ back to S, where $T_U^* = T_S$ and $c_2^* = c_3$. The login message $\{ID, T_U^*, c_2^*\}$ will pass the user authentication of Ku-Chen's scheme due to the fact that $c_2^* = c_3 = h(h(EID \oplus x) \oplus T_S)$. Finally, S responses the message $\{T_S^*, c_3^*\}$ to U, where $c_3^* = h(c_2^* \oplus T_S^*)$ and T_S^* is the current timestamp. The intruder U_a intercepts and drops this message.

B. Weakness in password change phase

When the smart card was stolen, unauthorized user can easily change new password of the card in password change phase. First, unauthorized user inserts U's smart card into the smart card reader of a terminal, enters ID and PW_a, where PW_a is unauthorized user's arbitrary password, and requests to change password. Next, unauthorized user enters arbitrary new password PW_a^* and then the smart card compute $R_{new}^* = R \oplus h(b \oplus PW_a) \oplus h(b \oplus PW_a^*)$, which yields
$$h(EID \oplus x) \oplus h(b \oplus PW) \oplus h(b \oplus PW_a) \oplus h(b \oplus PW_a^*),$$
and then replaces R with R_{new}^* without any checking. If malicious user stole the user U's smart card for a short time and change arbitrary new password like above mentioned, then the legal user U's succeeding login requests will be denied unless he re-registers to remote server again because $c_2 \neq h(hEID \oplus x) \oplus T_U)$ in verification phase. Therefore, Ku-Chen's password change phase is insecure.

IV. Proposed Scheme

A. Scheme

This section proposes an enhancement to Ku-Chen's scheme that can withstand the security flaws described in previous sections. The parallel session attack on Ku-Chen's scheme can succeed because U check $T_S = T_U$, but S did not check $T_S = T_U$. Ku-Chen's password change phase is insecure because the smart card replaces R with R_{new} without any checking. To resist above attacks, the proposed scheme performs as follows.

Registration: This phase is invoked whenever U initially registers or reregisters to S. Let n denote the number of times U re-registers to S.

1. U selects a random number b and computes $h(b \oplus PW)$.
2. $U \Rightarrow S$: ID, $h(b \oplus PW)$.
3. If it is U's initial registration, S creates an entry for U in the account database and stores $n = 0$ in this entry. Otherwise, S sets $n = n + 1$ in the existing entry for U. Next, S performs the following computations:
$$V = h(EID \oplus x)$$
$$R = h(EID \oplus x) \oplus h(b \oplus PW)$$
where $EID = (ID \| n)$.
4. $S \Rightarrow U$: a smart card containing V, R and $h()$.
5. U enters b into his smart card.

Note that U's smart card contains V, R, b, and $h()$, and U does not need to remember b after finishing Step 5.

Login: This phase is the same as in Ku-Chen's scheme.

Verification: After the authentication request message $\{ID, T_U, c_2\}$ is received, the remote system and the smart card execute the following operations.

1. If either ID or T_U is invalid or $T_S = T_U$, S rejects U's login request. Otherwise, S computes $h(h(EID \oplus x) \oplus T_U)$. If the computed result equals the received c_2, S accepts U's login request and computes $c_3 = h(h(EID \oplus x) \oplus T_S)$, where T_S denotes S's current timestamp. Otherwise, S rejects U's login request.
2. $S \rightarrow U$: T_S, c_3.
3. If either T_S is invalid or $T_S = T_U$, U terminates this session. Otherwise, U computes $h(c_1 \oplus T_S)$ and then compares the result to the received c_3. If equal, U successfully authenticates S.

Password Change: This phase is invoked whenever U wants to change his password PW with a new one, say PW_{new}.

1. U inserts his smart card into the smart card reader of a terminal, enters ID and PW, and requests to change password.
2. U's smart card computes $V^* = R \oplus h(b \oplus PW)$.
3. U's smart card verify V^* and stored V in smart card.
4. If they are equal, then U select new password PW_{new}, otherwise the smart card reject the password change request.
5. U's smart card compute $R_{new} = V^* \oplus h(b \oplus PW_{new})$ which yields $h(EID \oplus x) \oplus h(b \oplus PW_{new})$, and then replaces R with R_{new}.

B. Security analysis

In this section, we shall only discuss the enhanced security features. Rests are the same as original Ku-Chen's scheme in literature [2].

1. The proposed scheme can prevent the parallel session attack in Ku-Chen's scheme because the user and the remote server checks whether $T_S = T_U$, respectively.
2. The proposed password change phase is secure because the smart card verify V^* using stored V in Step 3 of the password change phase, when the smart card was stolen, unauthorized users cannot change new password of the card.

V. CONCLUSION

In the current paper, an enhancement to Ku-Chen's scheme was proposed. By compared with Ku-Chen's scheme, proposed scheme does not damage to the merits of their scheme. Moreover parallel session attack is completely solved and any legal users can select and change their password freely and securely. Therefore the proposed scheme is more secure.

REFERENCES

[1] H.Y. Chien, J. K. Jan and Y.M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, no. 4, pp. 372-375, 2002.

[2] W.C. Ku, and S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics,* vol. 50, no. 1, pp.204-207, February 2004.

[3] C. Mitchell, "Limitations of challenge-response entity authentication," *Electronics Letters*, vol. 25, no. 17, pp. 1195-1196, Aug. 1989.

[4] W.C. Ku, C.M. Chen, and H.L. Lee, "Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme," *IEICE Trans. Commun*., vol. E86-B, no. 5, pp. 1682-1684, May 2003.

[5] T. Hwang and W.C. Ku, "Reparable key distribution protocols for internet environments," *IEEE Trans. Commun.,* vol. 43, no. 5, pp. 1947-1950, May 1995.

[6] C.L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.

Eun-Jun Yoon received his BS in the School of Textile and Fashion Technology from the Kyung Il University, South Korea, and his MS in the Computer Engineering from the same University. He is now working toward the Ph.D. degree in the Kyungpook National University. His research interests include cryptography and network security.

Eun-Kyung Ryu received her MS in the Computer Engineering from the Kyungpook National University, South Korea. She is now working toward the Ph.D. degree in the same University. Her research interests include cryptography and network security.

Kee-Young Yoo received his BS degree in education of mathematics from Kyungpook National University in 1976; the MS degree in Computer Engineering from Korea Advanced Institute of Science and Technology in 1978 and the Ph.D. degree in the Computer Science from Rensselaer Polytechnic Institute, New York, U.S.A., in 1992. He is now a Professor at the Department of Computer Engineering, Kyungpook National University. His current research interests are wireless security and cryptography.