Cryptanalysis of two remote user authentication schemes using smart cards

Eun-Jun Yoon*, Eun-Kyung Ryu*, Young-Woo Jo*, and Kee-Young Yoo*
* Department of Computer Engineering, Kyungpook National University,
Daegu 702-701, Republic of Korea
{ejyoon, ekryu, hiro}@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract:

In 2004, Ku-Chen proposed an improvement to Chien et al.'s scheme to prevent from some weaknesses. Lee et al. also proposed an improvement to Chien et al.'s scheme to prevent from parallel session attack. This paper, however, will demonstrate that Ku-Chen's scheme is still vulnerable to the parallel session attack and Lee et al.'s scheme is also vulnerable to masquerading server attack.

Keywords: Authentication, Cryptography, Password, Parallel session attack, Masquerading server attack.

1. INTRODUCTION

In 1981, Lamport [1] proposed a remote user authentication scheme by using smart card. Following the conception of Lamport's scheme, many authentication schemes were proposed for enhancing the efficiency and security. In their schemes, the system has to maintain a password table for the user's authentication.

In 2002, Chien et al. [5] 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. However, Hsu [7] showed that Chien et al.'s scheme is vulnerable to the parallel session attack [3]. Recently, Ku-Chen [8] also pointed out that Chien et al.'s scheme is vulnerable to a reflection attack [2] and an insider attack [6]. In addition, they showed that Chien et al.'s scheme is not reparable [4] 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. Lee et al. [9] also proposed an improvement to Chien et al.'s scheme to prevent from parallel session attack proposed by Hsu [7]. This paper, however, will demonstrate that Ku-Chen's scheme is still vulnerable to the parallel session attack and Lee et al.'s scheme is also vulnerable to masquerading server attack.

This paper is organized as follows: In Section 2, we show that briefly review Ku-Chen's scheme and describe it suffer from vulnerability to the parallel session attack. In Section 3, we show that briefly review Lee et al.'s scheme and describe it suffer from vulnerability to masquerading server attack. Finally, conclusion is given in Section 4.

2. CRYPTANALYSIS 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.
- T_1 denotes the U 's current timestamp.
- T_2 denotes the S 's current timestamp.
- $\oplus$ denotes the bitwise XOR operation.
- $\Rightarrow$ represents a secure channel.
- $\rightarrow$ represents a common channel.

2.1 Review of Ku-Chen's Scheme

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

Registration phase: This phase is invoked whenever U initially registers or re-registers 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 phase: 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 computes $C_1 = R \oplus h(b \oplus PW)$ and $C_2 = h(C_1 \oplus T_1)$.
(3) $U \rightarrow S : ID, T_1, C_2$.

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

(1) If either ID or T_1 is invalid, S rejects U 's login request. Otherwise, S computes $h(h(EID \oplus x) \oplus T_1)$. If the computed result equals the received C_2, S accepts U 's login request and computes $C_3 = h(h(DIE \oplus x) \oplus T_2)$. Otherwise, S rejects U 's login request.
(2) $S \rightarrow U : T_2, C_3$.
(3) If either T_2 is invalid or $T_2 = T_1$, U terminates this session. Otherwise, U computes $h(C_1 \oplus T_2)$ and then compares the result to the received C_3. If equal, U successfully authenticates S.

Password Change phase: 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}.

2.2 Parallel session attack on Ku-Chen's Scheme

In the verification phase, consider the scenario of the parallel session attack that an attacker 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 $\{ID, T_1, C_2\}$ to S. If $\{ID, T_1, C_2\}$ is valid, the identification of U is authenticated and S responses $\{T_2, C_3\}$ to U. Once an attacker intercepts this message, he masquerades as the legal user U to start a new session with S by sending $\{ID, T_1^*, C_2^*\}$ back to S, where $T_1^* = T_2$ and $C_2^* = C_3$. The login message $\{ID, T_1^*, C_2^*\}$ will pass the user authentication of Ku-Chen's scheme due to the fact that $C_2^* = C_3 = h(h(EID \oplus x) \oplus T_2)$. Finally, S responses the message $\{T_2^*, C_3^*\}$ to U, where $C_3^* = h(C_2^* \oplus T_2^*)$ and T_2^* is the S 's current timestamp. The attacker intercepts and drops this message.

3. CRYPTANALYSIS OF LEE ET AL.'S SCHEME

3.1 Review of Lee et al.'s Scheme

There are three phases in Lee et al.'s scheme - registration, login and verification.

Registration phase: This phase is invoked whenever U initially registers or re-registers to S.

(1) $U \Rightarrow S : ID, PW$.
(2) S computes $R = h(ID \oplus x) \oplus PW$.
(3) $S \Rightarrow U$: a smart card containing R and $h()$.

Login phase: 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 computes $C_1 = R \oplus PW$ and $C_2 = h(C_1 \oplus T_1)$.
(3) $U \rightarrow S : ID, T_1, C_2$.

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

(1) If either ID or T_1 is invalid, S rejects U 's login request. Otherwise, S computes $h(h(ID \oplus x) \oplus T_1)$. If the computed result equals the received C_2, S accepts U 's login request and computes $C_3 = h(h(h(ID \oplus x) \oplus T_2))$. Otherwise, S rejects U 's login request.
(2) $S \rightarrow U : T_2, C_3$.
(3) If either T_2 is invalid, U terminates this session. Otherwise, U computes $h(h(C_1 \oplus T_2))$ and then compares the result to the received C_3. If equal, U successfully authenticates S.

3.2 Masquerading server attack on Lee et al.'s Scheme

In the login phase, if an attacker has intercepted and blocked the message transmitting in Step (3), i.e., $\{ID, T_1, C_2\}$, he can impersonate S to send $\{T_2^*, C_3^*\}$ to U in Step (2) of verification phase, where

$C_3^* = h(C_2)$ and $T_2^* = T_1$ is the current timestamp. Upon receiving the first item of the received message, i.e., T_2^*, U will compute $h(h(C_1 \oplus T_2^*))$. Note that Step (1) of verification phase is skipped by the attacker. Since the computed result equals the second item of the received message, i.e., C_3^*, U will be fooled into believing that the attacker is S. Since U can not actually authenticate S, Lee et al.'s scheme fails to provide mutual authentication as its authors claimed.

4. CONCLUSION

This paper, we have shown that Ku-Chen's scheme is vulnerable to the parallel session attack and Lee et al.'s scheme is vulnerable to masquerading server attack.

Acknowledgements

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

References

[1] L. Lamport, "Password authentication with insecure communication" Commun ACM, vol. 24, pp. 770-772, 1981.

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

[3] L. Gong, "A security risk of depending on synchronized clocks" Operation System Review, vol. 26, no. 1, pp. 49-53, 1992.

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

[5] 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.

[6] 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, 2003.

[7] 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.

[8] 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, 2004.

[9] S.W. Lee, H.S. Kim, and K.Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards" Computer Standards and Interfaces, in press, 2004.