Weaknesses of a Flexible Remote User Authentication Scheme Using Smart Cards

Wei-Chi Ku
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: wcku@csie.fju.edu.tw

Shuai-Min Chen
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: sean91@csie.fju.edu.tw

Hsiu-Mei Chuang
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: vivia@wcku1.csie.fju.edu.tw

Abstract-Recently, Lee, Hwang, and Yang proposed a verifier-free remote user authentication scheme using smart cards. Their scheme is efficient because of mainly using cryptographic hash functions. However, we find that Lee-Hwang-Yang's scheme is not reparable once the user's permanent secret is compromised and is vulnerable to a privileged insider's attack. Furthermore, it lacks the user eviction mechanism. In this paper, we first review Lee-Hwang-Yang's scheme, and then show its weaknesses.

Keywords: Password, Authentication, Reparability, Privileged insider's attack, User eviction.

1. Introduction

Password authentication is regarded as one of the simplest and most convenient user authentication mechanisms. A common feature of most conventional password authentication schemes is that a password verification table, which contains the verifiers of users' passwords, should be securely stored and maintained in the server. However, if the password verification table is stolen by the adversary, the system will be partially or totally breached. In 1990, Hwang, Chen, and Laih [8] proposed a non-interactive password authentication scheme and its enhanced version, which additionally uses smart cards. Their schemes are novel because the server neither requires storing verifiers nor keeping secrets of users. However, their original scheme and its enhanced version are flawed. Since then, many verifier-free password authentication schemes using smart cards have been proposed, and each has its pros and cons. In 1999, Yang and Shieh [22] proposed two verifier-free password authentication schemes using smart cards, one uses timestamps and the other uses nonces. However, their nonce-based scheme is inefficient while their timestamp-based scheme was found to be vulnerable to several forgery attacks [3], [7], [20]. Later, Fan, Li, and Zhu [7] proposed an improved version of Yang-Shieh's timestamp-based scheme. Unfortunately, Fan-Li-Zhu's scheme was found to be vulnerable to two forgery attacks [5], [21]. In 2000, Hwang and Li [10] proposed a verifier-free password authentication scheme using smart cards based on ElGamal's public-key technique. However, Hwang-Li's scheme does not allow users freely choosing and changing passwords. Furthermore, Hwang-Li's scheme was found to be vulnerable to various impersonation attacks [2], [4], [18], [23]. To overcome the security problems of Hwang-Li's scheme, Shen, Lin, and Hwang [18] proposed a modified scheme. However, the user's password is a pseudo-random number, and therefore is not easily memorable. Additionally, Shen-Lin-Hwang's scheme was found to be vulnerable to a forgery attack [16]. In 2003, Awasthi and Lal [1] proposed a verifier-free password authentication scheme using smart cards, and claimed that their scheme can achieve forward secrecy. In Awasthi-Lal's scheme, users can not freely choose and change passwords. In addition, Awasthi-Lal's scheme was found to be potentially vulnerable to a forgery attack [14].

All the schemes mentioned above require modular exponentiation operations and/or other heavy computations. To avoid using high-complexity operations such as modular exponentiation, Sun [19] proposed an efficient verifier-free password authentication scheme using smart cards based on cryptographic hash functions. The major drawbacks of Sun's scheme are that the password is not easily memorable and users can not freely choose and change passwords. Later, Chien, Jan, and Tseng [6] proposed a hash-based verifier-free password authentication scheme using smart cards to improve Sun's scheme.

However, Ku and Chen [13] pointed out that Chien-Jan-Tseng's scheme is vulnerable to a reflection attack and a privileged insider's attack, and is not reparable [9] once the user's permanent secret is compromised, and then described an improved version with better security. Independently, Lee, Hwang, and Yang [15] also proposed a hash-based verifier-free password authentication scheme using smart cards to improve Hwang-Li's scheme and Sun's scheme in that users can freely choose and change passwords. Unfortunately, we find that Lee-Hwang-Yang's scheme is not reparable and is vulnerable to a privileged insider's attack. Furthermore, it does not provide user eviction service. In this paper, we will describe the weaknesses of Lee-Hwang-Yang's scheme.

2. Review of Lee-Hwang-Yang's Scheme

For the reader's convenience, we first briefly describe Lee-Hwang-Yang's scheme before demonstrating its weaknesses. The notations used throughout this paper are summarized in Table 1.

Table 1. Notations of Lee-Hwang-Yang's scheme

notation	description
U	the user
S	the server
ID	U's identity
PW	U's password
x	S's permanent secret
$\oplus$	bitwise XOR operation
$h(\ )$	a public cryptographic hash function
T	current timestamp

Lee-Hwang-Yang's scheme involves four phases, the registration phase, the login phase, the authentication phase, and the password change phase, which can be described as in the following subsections.

2.1. Registration Phase

The registration phase is invoked once when U registers to S.

Step R1. U chooses his password PW and computes $h(PW)$, where $h(\ )$ is a public cryptographic hash function.

Step R2. U submits ID and $h(PW)$ to S for registration through a secure channel.

Step R3. S computes $PW_1 = h(ID \oplus x) \oplus h(PW)$.

Step R4. S delivers a smart card containing PW_1 and $h(\ )$ to U through a secure channel.

2.2. Login Phase

This phase is invoked whenever U requests to login S.

Step L1. U inserts his smart card into a login device and then enters ID and PW.

Step L2. U's smart card computes $h(PW)$ and $PW_2 = PW_1 \oplus h(PW)$, which yields $h(ID \oplus x)$, and then computes:

$$C_1 = h(PW_2 \oplus T)$$

where T denotes U's current timestamp.

Step L3. U sends $\{ID, C_1, T\}$ to S.

2.3. Authentication Phase

This phase is invoked whenever S receives U's login request. Let T' denote the timestamp S receives U's login request.

Step A1. If ID is invalid, S rejects U's login request.

Step A2. If $|T' - T| > \Delta T$, where ΔT denotes the maximal legal time interval for transmission delay, S rejects U's login request.

Step A3. S computes $h(h(ID \oplus x) \oplus T)$. If the computed result equals the received C_1, S accepts U's login request. Otherwise, S rejects U's login request.

2.4. Password Change Phase

This phase is invoked whenever U requests to change his password PW with a new one PW^*.

Step P1. U inserts his smart card into a login device, and then enters ID, PW, and PW^*.

Step P2. U's smart card first computes $h(PW)$ and $h(PW^*)$, and then computes $PW_2 = PW_1 \oplus h(PW)$, which yields $h(ID \oplus x)$. Next, U's smart card computes the following item:

$$PW_1^* = PW_2 \oplus h(PW^*)$$

Step P3. U's smart card replaces PW_1 with PW_1^*.

3. Weaknesses of Lee-Hwang-Yang's Scheme

In this section, we will show that Lee-Hwang-Yang's scheme is not reparable and is vulnerable to a privileged insider's attack. Furthermore, it lacks the user eviction mechanism.

3.1. Poor Reparability

Although the tamper resistance of smart cards is widely assumed, however, such an assumption may be problematic in practice. Actually, many researches have showed that the secrets stored in a smart card can be breached by monitoring the power consumption, e.g., [11], or analyzing the leaked information, e.g., [17]. Suppose that the adversary has obtained the PW_1 stored in U's smart card and also intercepted the message transmitted in Step L3, i.e., $\{ID, C_1, T\}$, during one of U's past login processes. Then, the adversary can perform a guessing attack to obtain PW as follows. The adversary guesses a candidate password PW' and computes

$$PW_2' = PW_1 \oplus h(PW') = h(ID \oplus x)'$$
$$C_1' = h(PW_2' \oplus T)$$

If C_1' equals the intercepted C_1, the adversary has correctly guessed $PW' = PW$, which also implies that he has obtained $PW_2' = PW_2$ $(= h(ID \oplus x))$. Otherwise, the adversary tries another candidate password. After obtaining PW_2, the adversary can use it to impersonate U to login S. Unfortunately, such a fraud can not be prohibited even if U has detected that his PW_2 has been compromised and then uses a new password PW^* to request for re-registration. As PW_2 is uniquely determined by U's identity ID and S's permanent secret key x, S can not change PW_2 for U unless either ID or x can be changed. However, since x is commonly used for all users rather than specifically used for only U, it is unreasonable and inefficient if x should be changed to recover the security for U only. Furthermore, it is also impractical to change ID, which should be tied to U uniquely in most application systems. Hence, the adversary can still employ the compromised PW_2 to impersonate U to login S. That is, Lee-Hwang-Yang's scheme is not reparable [9].

3.2. Privileged Insider's Attack

In real environments, it is likely that the user uses the same password to access several servers for his convenience. In this case, if a privileged insider of the server, e.g., the administrator, has learned the user's password, he may try to impersonate the user to access other servers [12]. In the registration phase of Lee-Hwang-Yang's scheme, the hashed value of U's password PW, i.e., $h(PW)$, will be revealed to S after Step R2. The privileged insider of S can guess a candidate password PW' and compute $h(PW')$. If the computed result equals $h(PW)$, the privileged insider of S has correctly guessed $PW' = PW$. Otherwise, the privileged insider of S tries another candidate password. Knowing PW, the privileged insider of S can try to use it to impersonate U to access other servers. Although it is also possible that all the privileged insiders of S are not malicious and U does not use the same password to access several servers, the implementers and the users of the scheme should be aware of such a potential weakness.

3.3. No Eviction Mechanism

When a user is evicted from the server, there should be a mechanism that can be used to revoke all the accessing rights assigned to him. In Lee-Hwang-Yang's scheme, if U is evicted from S, he can still login S because S can not distinguish the evictee from the users that are not evicted. If S has to maintain a blacklist to record all the evictees, it violates the original expectation for Lee-Hwang-Yang's scheme that the server does not need to store any user related information except his own secret key x for authenticating the user.

4. Conclusion

We have shown that a flexible remote user authentication scheme proposed by Lee, Hwang, and Yang is not reparable once the user's permanent secret is compromised and is vulnerable to a privileged insider's attack. It should be emphasized that the secrets of the system can not be guaranteed secure all the time in real environments. Therefore, there should be some mechanism that can effectively and efficiently remove the breach resulted from the compromised secrets. Furthermore, we have pointed out that Lee-Hwang-Yang's scheme does not provide the user eviction service. Unfortunately, as we know, none of existing verifier-free password authentication schemes provides the user eviction service. It deserves further research to solve this problem.

Acknowledgment

This work was partly supported by the National Science Council, R.O.C., under Grant NSC-93-2213-E-030-017.

References

[1] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246–1248, Nov. 2003.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 992–993, Nov. 2000.

[3] C. K. Chan and L. M. Cheng, "Cryptanalysis of a timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 1, pp. 74–76, 2002.

[4] C. C. Chang and K. F. Hwang, "Some forgery attacks on a remote user authentication scheme using smart cards," *Informatica*, vol. 14, no. 3,

pp. 289–294, 2003.

[5] K. F. Chen and S. Zhong, “Attacks on the (enhanced) Yang-Shieh authentication,” *Computers & Security*, vol. 22, no. 8, pp. 725–727, Dec. 2003.

[6] 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.

[7] L. Fan, J. H. Li, and H. W. Zhu, “An enhancement of timestamp-based password authentication scheme,” *Computers & Security*, vol. 21, no. 7, pp. 665–667, Nov. 2002.

[8] T. Hwang, Y. Chen, and C. S. Laih, “Non-interactive password authentications without password tables,” *Proc. IEEE Region 10 Conference on Computer and Communication Systems*, Hong Kong, pp. 429–431, Sept. 1990.

[9] T. Hwang and W. C. Ku, “Reparable key distribution protocols for Internet environments,” *IEEE Transactions on Communications,* vol. 43, no. 5, pp. 1947–1950, May 1995.

[10] M. S. Hwang and L. H. Li, “A new remote user authentication scheme using smart card,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[11] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” *Proc. Advances in Cryptology* (CRYPTO’99), pp. 388–397, 1999.

[12] W. C. Ku, C. M. Chen, and H. L. Lee, “Cryptanalysis of a variant of Peyravian-Zunic’s password authentication scheme,” *IEICE Transactions on Communications*, vol. E86-B, no. 5, pp. 1682–1684, May 2003.

[13] 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, Feb. 2004.

[14] W. C. Ku, S. M. Chen, and H. M. Chuang, “A study of hash-based password authentication schemes without storing verifiers,” *Proc. 14th Information Security Conference*, Taiwan, pp. 429–435, June 2004.

[15] C. C. Lee, M. S. Hwang, and W. P. Yang, “A flexible remote user authentication scheme using smart cards,” *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46–52, July 2002.

[16] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, “Cryptanalysis of a modified remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243–1245, Nov. 2003.

[17] 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*, vol. 51, no. 5, pp. 541–552, May 2002.

[18] J. J. Shen, C. W. Lin, and M. S. Hwang, “A modified remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, May 2003.

[19] H. M. Sun, “An efficient remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, Nov. 2000.

[20] H. M. Sun and H. T. Yeh, “Further cryptanalysis of a password authentication scheme with smart cards,” *IEICE Transactions on Communications*, vol. E86-B, no. 4, pp. 1412–1415, April 2003.

[21] B. Wang, J. H. Li, and Z. P. Tong, “Cryptanalysis of an enhanced timestamp-based password authentication scheme,” *Computers & Security*, vol. 22, no. 7, pp. 643–645, Oct. 2003.

[22] W. H. Yang and S. P. Shieh, “Password authentication schemes with smart cards,” *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

[23] H. T. Yeh, H. M. Sun, and B. T. Hsieh, “Security of a remote user authentication scheme using smart cards,” *IEICE Transactions on Communications*, vol. E87-B, no. 1, pp. 192–194, Jan. 2004.