Weaknesses of a Remote User Password Authentication Scheme Using Smart Card

Debiao He, Jianhua Chen, and Jin Hu
(Corresponding author: Debiao He)

School of Mathematics and Statistics, Wuhan University, Wuhan, Hubei 430072, China
No.483, Bayi Rd., Wuchang District, Wuhan 430072, China (Email:hedebiao@163.com)

(Received Dec. 9, 2009; revised and accepted Mar. 29, 2010)

Abstract

Remote authentication is a method to authenticate remote users over insecure communication channel. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. Very recently, Hsiang et al. pointed out that Yoon et al's scheme is vulnerable to parallel session attack, masquerading attack and password guess attack. They proposed an improved scheme to remedy these pitfalls. They claimed their scheme can against parallel session attack, masquerading attack and password guess attack. However, we find that Hsiang et al.'s scheme is vulnerable password guess attack, masquerading user attack and masquerading server attack.

Keywords: Attacks, authentication, cryptanalysis, security, smart card

1 Introduction

Remote authentication is a method to authenticate remote users over insecure communication channel. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. In 1981, Lamport [8] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. Since then, many password-based authentication schemes were proposed to improve the security, efficiency or cost [1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 14].

In 2000, Huang et al. [3] presented a password-based remote user authentication scheme using smart cards. However, Chien et al. [1] found Huang et al.'s scheme could not withstand masquerade attack and proposed an efficient password based remote user authentication scheme. In 2003, Ku et al. [6] pointed out that Chien et al.'s scheme is vulnerable to a reflection attack, inside attack, and is not reparable. Ku et al. also proposed an improved scheme to eliminate the security vulnerability of Chien et al.'s scheme. Yoon et al. [14] found that Ku et al.'s scheme was still susceptible to parallel session attack and insecure for changing the user's password in password change phase. Yoon et al. also developed an improved scheme.

Very recently, Hsiang et al. [2] pointed out that Yoon et al's scheme is vulnerable to parallel session attack, masquerading attack and password guess attack. They proposed an improved scheme to remedy these pitfalls. They claimed their scheme can against parallel session attack, masquerading attack and password guess attack. However, we find that Hsiang et al.'s scheme is vulnerable password guess attack, masquerading user attack and masquerading server attack.

The rest of the paper is organized as follows: Section 2 briefly reviews Hsiang et al.'s scheme. Section 3 elaborates the cryptanalysis of their scheme. At the end, Section 4 concludes this paper.

2 Review of Hsiang et al.'s Scheme

The notations used throughout this paper are described as in the following.

- U: a user.
- ID_u, PW_u: U's identifier and password, respectively.
- $CARD$: U's smart card.
- S: a remote server.
- x: S's secret key.
- T_U, T_S: U's current timestamp and S's current timestamp, respectively.
- $h(\cdot)$: a hash function.
- $\oplus$: bitwise XOR operation.
- $X \rightarrow Y\{M\}$: X sends a message M to Y over a common communication channel.

Hsiang et al.'s scheme, involves four phases, the registration phase, the login phase, the verification phase, and the password change phase, which can be described as in the following.

Registration phase. In this phase, the user U initially registers with the server S.

1) U chooses his ID_U, PW_U and a random number b, then computes $h(PW_U)$ and $h(b \oplus PW_U)$. At last, U sends $ID_U, h(PW_U)$ and over a secure communication channel to S.

2) Upon receiving ID_U, $g(PW_U)$ and $h(b \oplus PW_U)$, S checks if it is U's first registration. If it is, creates an entry for in the account database and stores $n = 0$ in the entry. Otherwise, S sets $n = n + 1$ in the existing entry for U. Next, S computes $EID_U = h(ID_U \parallel n)$, $P = h(EID_U \oplus x)$, $R = P \oplus h(b \oplus PW_U)$, and $V = h(P \oplus h(PW_U))$. At last, S stores the secure information V, R and $h(\cdot)$ into U's smart card $CARD$ and gives the smart card to U.

3) Upon receiving $CARD$, U enters b into his smart card.

Login phase. In this phase, the user U sends a login request message to the server S whenever U wants to access some resources upon S.

1) U inserts his smart card, $CARD$, into a smart card reader and then inputs his ID_U and PW_U.

2) Using PW_U, the smart card computes $C_1 = R \oplus h(b \oplus PW)$ and $C_2 = h(C_1 \oplus T_U)$, where T_U is the current timestamp.

3) $U \rightarrow S\{ID, T_U, C_2\}$.

Verification phase. In this phase, the server S verifies the authenticity of the login message requested by the user U.

1) Upon receiving the message ID, T_U, C_2, S checks ID_U and T_U. If either ID_U or $T_s - T_U \leq 0$. S rejects U's login request. Otherwise, S computes $h(h(EID_U \oplus x) \oplus T_U)$. 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 is S's current timestamp. Otherwise, S rejects U's login request.

2) $S \rightarrow U\{T_S, C_4\}$.

3) Upon receiving the message $\{T_S, C_3\}$, U checks T_S. If T_S is invalid or equals T_U, U terminates this session. Otherwise, U computes $h(C_1 \oplus T_S)$, then compares the result to the received C_3. If equal, U successfully authenticates S.

Password change phase. In this phase, the user U changes his password any time he wants.

1) U inserts his smart card into a smart card reader and then types in his ID_U and PW_U.

2) The smart card computes $P^* = R \oplus h(b \oplus PW)$ and $V^* = h(P^* h(PW_U))$.

3) The smart card compares V^* with the stored V in smart card. If they are not equal, the smart card rejects the password change request. Otherwise, U chooses a new password PW'_U.

4) The smart card then computes $R' = R \oplus h(b \oplus PW'_U)$ and V. It now replaces R and V with newly updated R' and V', respectively.

3 Weaknesses Analysis of Hsiang et al.'s Scheme

We assume that an attacker A has total control over the communication channel between the user U and the remote server S, which means that he can insert, delete, or alter any messages in the channel. According to the researches in [5, 11], all existing smart cards are vulnerable since the secret values stored in a smart card could be extracted by monitoring its power consumption. Therefore, we further assume that the attacker A can steal the user's smart card and extract the values stored in the smart card. Under these two assumptions, we will examine some weaknesses of Hsiang et al.'s remote user authentication method.

3.1 Password Guess Attack

In Hsiang et al.'s scheme, V, R, b, and $h(\cdot)$ are stored in the smart card after registration. It's easy to say that there is the following relation between V, R and b about PW_U.

$$V = h(R \oplus h(b \oplus PW_U) \oplus h(PW_U)).$$

Then the adversary can carry out the off-line password guessing attack using the relation. The detailed description of the attack is as follows. Fist, A get the value of V, R and b using the method in [5, 11]. Then A can carry out the password guess attack using V, R and b. The process of the off-line password guessing attack is as follows.

1) A selects a password PW's from a uniformly distributed dictionary D.

2) A computes $V' = h(R \oplus h(b \oplus PW') \oplus h(PW'))$.

3) A then verify the correctness of PW' by checking that V' is equal to V.

4) A repeats steps 1, 2, and 3 of this phase until the correct password if found.

3.2 Masquerading User Attack

Once the adversary A obtained PW through above attack, he/she can get the value P by computing $P = R \oplus h(b \oplus PW_U)$. A can forge U's login message by computes $C_2 = g(P \oplus T'_U)$, and sending ID, T_U and C_2 to S, where T'_U is current timestamp. It is easy to say the forged message can pass S's verification. Hence, Hsiang et al.'s scheme is vulnerable to masquerading user attack.

3.3 Masquerading Server Attack

Once the adversary A obtained the value P by the above method, he can masquerade the serve as follows.

Upon intercepting the message ID, T_U and C_2, A computes $C_3 = h(P \oplus h(T'_S))$, where T'_S is the current timestamp. Then A masquerades the server S and sends $\{T'_S, C_3\}$ to the user U. It's easy to say that the message T'_S, C_3 can pass U's verification. Hence, S.-K. Kim et al.'s scheme is vulnerable to masquerading server attack.

4 Conclusion

Smart card-based user authentication technology has been widely deployed in various kinds of applications, such as remote host login, withdrawals from automated cash dispensers, and physical entry to restricted areas. In 2009, Hsiang et al. proposed a mutual authentication scheme using smart cards and showed their scheme can against parallel session attack, masquerading attack and password guess attack. However, we have demonstrated that Hsiang et al.'s scheme is vulnerable password guess attack, masquerading user attack and masquerading server attack. For this reason, Hsiang et al.'s scheme is insecure for practical application. It is important that security engineers should be made aware of this, if they are responsible for the design and development of smart card-based user authentication systems.

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] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," *Computer Communications*, no. 32, pp. 649-652, 2009.

[3] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.

[4] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematicaland Computer Modeling*, vol. 36, no. 1-2, pp. 103-107, 2002.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology (Crypto'99)*, pp. 388-397, Santa Barbara, USA, 1999.

[6] 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.

[7] M. Kumar, "A New Secure Remote User Authentication Scheme with Smart Cards," *International Journal of Network Security*, vol. 11, no. 2, pp. 88-93, 2010.

[8] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, no. 24, pp. 770-772, 1981.

[9] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks, " *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727-740, 2006.

[10] K. V. Mangipudi and R. S. Katti, "A hash-based strong password authentication protocol with user anonymity," *International Journal of Network Security*, vol. 2, no. 3, pp. 205-209, 2006.

[11] 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, 2002.

[12] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and key issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101-115, 2006.

[13] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards," *International Journal of Network Security*, vol. 3, no. 3, pp. 283-285, 2006.

[14] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612-614, 2004.

Debiao He received his Ph.D. degree from School of Mathematics and Statistics, Wuhan University. He is currently an instructor of School of Mathematics and Statistics, Wuhan University. His research interests include cryptology and nformation security.

Jin Hu received the B.Sc.and M.Sc.degrees in applied mathematics from Wuhan University, China, in 2002 and 2005, respectively. He is now a PhD candidate in the School of Mathematics and Statistics, Wuhan University. His research areas include information security and biomedical imaging.

Jianhua Chen received his Ph.D. degree from School of Mathematics and Statistics, Wuhan University. His is currently a professor with School of Mathematics and Statistics, Wuhan University. His research interests include cryptology and information security.