SECURE USER-FRIENDLY REMOTE AUTHENTICATION SCHEMES

Tzung-Her CHEN, Du-Shiau TSAI, and Gwoboa HORNG

Abstract: Recently, Hwang and Li proposed a remote user authentication scheme that does not require a password table to verify the legitimacy of a legal user.[1] This method uses smart cards. To benefit from this advantage, other research works have explored adding such features as reducing the computational cost, adopting user-friendly passwords, making it easier to change user passwords, etc. However, as cryptanalysis has evolved, a series of modifications that improve the known security flaws have been made subsequently. This article deals with a security problem found in a latest modification and improves it in order to construct a more secure function. The article also highlights a feature, mutual authentication between a server and users, found in many authentication protocols but seldom found in the considered series of modifications.

Keywords: Mutual Authentication, Remote Authentication, Smart Card, User Impersonation.

Introduction

Nowadays, we can transfer money and shop using e-commerce applications. It could be predicted that, with network support, more activities will be performed without the need for a face to face contact. Hence, authentication has become one of the most significant and challenging issues in Internet commerce.

Remote authentication is the process through which one proves and verifies certain information over networks. Password-based remote authentication is one of the most commonly used authentication techniques due to its simplicity and effectiveness.

Authentication schemes generally use a password/ verification table stored at the server side. This stored-table system can easily suffer from verifier-stolen or modification attacks. Clearly, a more secure way that requires no password/ verification in the server to verify user legitimacy is required. Therefore, ID-based [2] authentication schemes [3,4] have been proposed to remove the requirement of having a password/ verification table stored on the server.

Hwang and Li have proposed a remote user authentication scheme using smart cards.[5] The main advantage is that a password table is not required to verify a user's legitimacy. Unfortunately, several security flaws have been identified in their method.[6,7,8,9]

Inspired by the scheme proposed by Hwang and Li, Sun [10] has presented an efficient scheme with two main advantages: (1) low communication and computation costs and (2) no password table required. Unfortunately, the user password is computed by the server and is too lengthy to be memorized easily. Hwang [11] and Chien [12] have independently proposed hash-function-based schemes with much lower computation than before. However, Hwang's scheme does not provide mutual authentication, while the scheme proposed by Chien provides mutual authentication but suffers from the parallel session attack.[13] A scheme proposed by Wu and Chieu [14] in 2003, focuses on user friendliness, allowing the users to freely choose and change their passwords.

This article first determines the security flaw in the Wu-Chieu's scheme and then eliminates it to form a new approach (named shortly Method 1). Second, the authors propose another scheme (Method 2) to highlight a feature, mutual authentication between a server and remote users, found in many authentication protocols but seldom addressed in the considered approaches.

The remainder of this paper is organized as follows. In the next section, the Wu-Chieu's scheme is briefly described and its security flaw outlined. Two enhancements are proposed afterwards. This is followed by a discussion and security analysis. Conclusions are given in the last section.

Review and Weakness of Wu-Chieu's Scheme

The Wu-Chieu's password authentication scheme consists of three phases [15]: registration, login, and authentication phases.

Registration Phase

Step R.1 $U \rightarrow S : ID, PW$

In the registration phase, a user U sends his/her identity ID and password PW to the server S through a secure channel.

Step R.2 $S \rightarrow U$: smart card $\{ID, A, B, h(.), p, q\}$

Upon receiving the registration request, the server computes the following values:

- $A = h(ID, x)$, where x is the server's secret key and $h(.)$ is a collision resistant one-way function.

- $B = g^{A \cdot h(PW)} (\bmod \mathrm{p})$ where p is a large prime number, and g is a primitive element in $\mathrm{GF}(p)$.

The server then writes $\{ID, A, B, h(.), p, q\}$ into the user's smart card and releases it to the user.

Login Phase

Step L.1 $U \to S : ID, B^*, C, T$

In the login phase, user U inserts his/her smart card into a login device and enters his/her PW^*. The smart card will calculate the following values:

- $B^* = g^{A \cdot h(PW^*)} (\bmod \mathrm{p})$
- $C = h(T \oplus B)$, where T is the current date and time and $\oplus$ is the exclusive-OR operation.

The client then sends the login message $\{ID, B^*, C, T\}$ to the remote system.

Authentication Phase

Upon receiving the login message at time T', the server performs the following operations:

- Checks the format of ID.
- Checks the time interval validation between T and T'; whether $(T' - T) \geq \Delta T$ (the expected valid time interval for transmission delay). If the time interval is invalid the system rejects the login request.
- Computes $C^* = h(T \oplus B^*)$ and checks if C^* is equal to the received C. If it holds, it implies that the input PW^* is equal to PW and the user is authenticated; otherwise, this login request is rejected.

Security of Wu-Chieu's Scheme

In the Wu-Chieu's scheme, a user requesting login is authenticated if his/her login message $\{ID, B^*, C, T\}$ satisfies $C = h(T \oplus B^*)$. No one is able to forge $C = h(T \oplus B) = h(T \oplus g^{A \cdot h(PW)})$ due to the fact that C has to be derived from PW and A, calculated from the server secret key x.

The authors will demonstrate below that an attacker can impersonate a legal user and pass server authentication by successfully forging the login message using the following methods:

Attack 1

Assume that an attacker has intercepted the last login message $\{ID, B^{*}, C, T\}$. Now, s/he calculates $C^{**} = h(T^{**} \oplus B^{*})$, where T^{**} is the current date and time. Then s/he sends $\{ID, B^{*}, C^{**}, T^{**}\}$ to the remote server.

After receiving the login request, the server computes $C^{***} = h(T^{**} \oplus B^{*})$ and checks if C^{***} is equal to the received C^{**}. Unfortunately, it holds and the attacker is authenticated.

Attack 2

An even simpler attack can be launched by first computing $c = h(T \oplus b)$, where b is a randomly selected number and t is the current date and time. Then $\{ID, b, c, t\}$ is sent to the remote server as a login message.

After receiving the login message, the server computes $C = h(T \oplus b)$ and checks if C is equal to the received c. Unfortunately, this will hold and an attacker will be authenticated.

The Proposed Schemes

In this section, a secure enhanced scheme is proposed as Method 1 to improve the security of the Wu-Chieu's scheme. The seldom addressed issue, mutual authentication, will be highlighted and solved in Method 2.

The Proposed Security Enhancement (Method 1)

First, an improved version of the Wu-Chieu's scheme is described below.

The *registration phase* goes as follows.

Step R.1 $U \to S : ID, h(PW)$

A user U sends his/her identity ID and the hash value of the password PW to the server S in a secure way.

Step R.2 $S \to U$: smart card $\{ID, A, B, h(.), p, q\}$

Upon receiving the registration request, the server computes the following values:

- $A = h(ID, x)$.
- $B = g^{A \cdot h(PW)} (\text{mod p})$.

Then the server writes $\{ID, A, B, h(.), p, q\}$ into the user's smart card and releases it to the user.

The *login phase* goes as follows.

Step L.1 $U \rightarrow S : ID, B^*, C, T$

The user U inserts his/her smart card into a login device and enters his/her password PW^*. The smart card will calculate the following values:

- $B^* = g^{A \cdot h(PW^*)} (\bmod \mathrm{p})$.
- $C = h(T \oplus B \oplus A)$, where T is the current date and time.

The client then sends the login message $\{ID, B^*, C, T\}$ to the remote server.

Upon receiving the login message at time T', the server performs the following operations:

- Checks the format of ID and the validation of the time interval between T and T'.
- Computes $C^* = h(T \oplus B^* \oplus h(ID, x))$, and checks if C^* is equal to the received C. If it holds, it implies that the input PW^* is equal to PW and the user is authenticated; otherwise, this login request is rejected.

In case the user wants to change his/her password, the following operations are performed.

- The user inputs his new password PW^*.
- The smart card computes new $B = g^{A \cdot h(PW^*)} (\bmod \mathrm{p})$ and updates it.

The Proposed Scheme with Mutual Authentication (Method 2)

Although Method 1 enhances the security of the Wu-Chieu's scheme, it does not provide mutual authentication. Method 2 addresses this issue. The registration phase is the same as that of Method 1 and will be omitted here. The login phase goes as follows.

Step L.1 $U \rightarrow S : ID, B^*, C_1, C_2, T$

U inserts his/her smart card into a login device and enters his/her PW^*. The smart card will calculate the following values:

- $B^* = g^{A \cdot h(PW^*)} (\bmod \mathrm{p})$.

- $C_1 = h(T \oplus B \oplus A)$, where T is the current date and time.
- $C_2 = r \oplus A$, where r is a random number as a challenge for the remote server.

Step L.2 $S \rightarrow U : h(r)$

Upon receiving the login message at the time T', the server performs the following operations:

- Checks the format of ID and the validation of the time interval between T and T'.
- Computes $C_1^* = h(T \oplus B^* \oplus h(ID, x))$, and checks if C_1^* is equal to the received C_1. If it holds, it implies that the input PW^* is equal to PW and the user is authenticated; otherwise, this login request is rejected.
- Extracts r from C_2 using $h(ID, x)$.
- Computes and sends $h(r)$ to the user as a response.

Upon receiving $h(r)$, the user checks the validation of $h(r)$. If it holds, the server is authenticated. The user is convinced that the server, which he is going to communicate with, is a regular one.

The change of the user password is the same as in Method 1 and will not be described here.

Discussion and Security Analysis

In Method 1, the proposed scheme replaces $C = h(T \oplus B)$ in the login phase of the Wu-Chieu's scheme with $C = h(T \oplus B \oplus A)$. Hence, an attacker has no efficient way to forge C, which equals $C = h(T \oplus B \oplus A)$, without knowing A, protected by the smart card.

In Method 2, the identity of the user is verified by checking if the hash value of $T \oplus B^* \oplus h(ID, x)$ is equal to the received C_1 in Step L.1. The identity of the server is verified by checking if the server possesses the secret key x to generate $A = h(ID, x)$ and uses A to extract r from C_2. If the user receives the server response $h(r)$, it implies that authentication for the server is indirectly proved since only both the legal user and the regular server know A or $h(ID, x)$.

The advantages of the proposed schemes in terms of adding important functions can be summarized as follows.

- *Reducing computation cost*: In the login and authentication phases, the proposed schemes need one modular exponential operation (similarly to the Wu-Chieu's scheme), while five operations are required in the scheme proposed by Hwang and Li.[16] The methods proposed by Chien, Jan, and Tseng,[17] Hwang, Lee, and Tang,[18] and Sun [19] do not require modular exponential operations other than one-way hash functions. The computation cost for a secure one-way hash function is not yet addressed clearly; however, it is widely believed that one-way functions exist [20] and its computation cost is lower than that of a modular exponential operation. In fact, no function has been found that is really a one-way yet. Modular exponentiation is well-regarded as a candidate for a one-way function.
- *Eliminating verification table*: The proposed schemes do not require a password/ verification table to verify the users. Hence, it provides higher security level of the system and reduces cost of maintaining the sensitive tables on the server.
- *Securing password from server*: If the server knows the user password, it is possible that the server will impersonate a legal user, an especially sensitive issue in such applications as electronic accounting, electronic transfer, etc. In the proposed schemes, the user sends in the registration phase $h(PW)$ to the server but not PW . It reduces the possibility of revealing PW to the server.
- *Choosing friendly password*: Passwords are useful if kept secret, in providing additional security protection in case the smart card is lost. If a password is not convenient to use or not friendly, it will not be used at all or it will be used incorrectly. Hence, the proposed schemes provide also this feature.
- *Changing password easily*: The proposed schemes offer this alternative function to facilitate simplicity, friendliness and effectiveness.
- *Providing mutual authentication*: Most authentication schemes provide only unilateral authentication, making it is possible for an attacker to impersonate the server to fool the legal user into divulging security information. In some situations, mutual authentication is an important feature with a higher security level.

Table 1 compares the proposed schemes with several related schemes.

Remote authentication schemes could be attacked from the client side, in the transmission channel, and from the server side. This is in addition to password-guessing attacks. In the transmission channel, an attacker can intercept or modify the login message between the user and the server and pretend that s/he is the user or the server.

Table 1: Functional Comparisons among a Series of Related Remote User Authentication Schemes.

	Hwang-Li [21]	*Sun* [22]	*Wu-Chieu* [23]	*Tang-Lee-Hwang* [24]	*Chien-Jan-Tseng* [25]	*Proposed Method* 2
Computation	Medium	Extremely Low	Low	Extremely Low	Extremely Low	Low
Verification table	No	No	No	No	No	No
Server - know password	Yes	Yes	Yes	No	Yes	No
Friendly password	No	No	Yes	Yes	Yes	Yes
User - change password	No	No	Yes	Yes	No	Yes
Mutual authentication	No	No	No	No	Yes	Yes

From the client side, an attacker could impersonate a legal user to login to the server (user impersonation attacks) or merely replay the intercepted login message (replay attacks).

From the server side s/he may impersonate the server to fool a legal user (server impersonation attacks); or modify the authentication message to cheat the server. Of course, an attacker may find other ways to steal the password/ verification table stored on the server (verifier-stolen attacks) to guess a password, perform impersonation operations or just modify the table (modification attacks) to deny legal users from being able to successfully login.

To demonstrate the work of the proposed schemes, in what follows the authors will present the possible attacks against password authentication scheme.

Password Guessing Attacks

The login message is $B^* = g^{A \cdot h(PW^*)}$. If an attacker intercepts B^*, it is not possible to guess the user password without knowing A since s/he has no feasible way to determine the correct password.

User Impersonating Attacks

In Method 1, an attacker may impersonate a legal user by forging a login request $\{ID, B^*, C, T\}$. Due to the fact that the server checks the $T \oplus B^* \oplus h(ID, x)$ hash value an attacker must have $h(ID, x)$ or A to compute $C = h(T \oplus B^* \oplus h(ID, x))$ in Step L.1 so as to pass authentication. However, s/he has no idea about the server’s secret key x to obtain $h(ID, x)$. The attacker will have no efficient way to find A from $C = h(T \oplus B^* \oplus A)$ or $B^* = g^{A \cdot h(PW^*)}$ due to the NP-hardness of the problem of breaking one-way hash functions and solving discrete logarithm.

Similarly, in Method 2, the attacker cannot extract A from $C_2 = r \oplus A$. He faces the same challenge of not knowing the server's secret key x.

Replay Attacks

The login message is refreshed for each login phase by introducing a timestamp. Hence, in both Methods 1 and 2, an attacker cannot login to the remote server by replaying a previous login message.

Server Impersonating Attacks

Method 1 focuses on how to verify the identity of a user for a server, but not on verifying the legality of a server. This attack is not discussed here.

In Method 2, if an attacker attempts to impersonate the remote server successfully, he must send the exact $h(r)$ to the client (see Step L.2 in Method 2). The client will compute the hash value of r and compare it with the received $h(r)$. If equal, server authentication will be successful. This implies that the attacker has to extract r from C_2. He cannot extract r for the reason that he faces an NP-hard computation problem.

Verifier-Stolen Attacks & Modification Attacks

Because no password/ verification table is stored on the server, verifier-stolen and modification attacks are not possible.

Conclusions

Friendly passwords are very useful, if kept secret, in protecting from theft by providing another defense line. To avoid the risk of revealing any sensitive information from the password/ verification table, it is a better strategy to eliminate the sensitive table from the server. Two solutions have been proposed in this paper. The first proposed password authentication scheme removes the sensitive table security flaw from the server. The second proposed scheme adds a mutual authentication feature. Compared with other related schemes, the proposed schemes provide higher security. The authors have demonstrated that the proposed schemes are reliable and secure.

Notes:

[1] Min-Shiang Hwang and Li-Hua Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 46, no. 1 (February 2000): 28-30.

[2] Shigeo Tsujii and Toshiya Itoh, "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem," *IEEE Journal on Selected Areas in Communications* 7, no. 4 (May 1989): 467-473.

[3] Chin-Chen Chang and Shin-Jia Hwang, "Using Smart Cards to Authenticate Remote Passwords," *Computers and Mathematics with Applications* 26, no. 7 (1993): 19-27.

[4] Chin-Chen Chang and Tzong-Chen Wu, "Remote Password Authentication with Smart Cards," *IEE Proceedings – Part E* 138, no. 3 (1991): 165-168.

[5] Hwang and Li, "A New Remote User Authentication Scheme Using Smart Cards."

[6] Chi-Kwong Chan and L.M. Cheng, "Cryptanalysis of a Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 46, no. 4 (November 2000): 992-993.

[7] Chin-Chen Chang and Kuo-Feng Hwang, "Some Forgery Attacks on a Remote User Authentication Scheme Using Smart Cards," *Informatica* 14, no. 3 (2003): 289-294.

[8] Kai-Chi Leung, L.M. Cheng, Anthony S. Fong, and Chi- Kwong Chan, "Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 49, no. 4 (November 2003): 1243-1245.

[9] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards," IEEE *Transactions on Consumer Electronics* 49, no. 2 (May 2003): 414-416.

[10] Hung-Min Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 46, no. 4 (November 2000): 958-961.

[11] Yuan-Liang Tang, Cheng-Chi Lee, and Min-Shiang Hwang, "A Simple Remote User Authentication Scheme," *Mathematical and Computer Modelling* 36 (2002): 103-107.

[12] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Computers & Security* 21, no. 4 (2002): 372-375.

[13] Chien-Lung Hsu, "Security of Chien et al.'s Remote User Authentication Scheme Using Smart Cards," *Computer Standards and Interfaces* 26, no. 3 (2004): 167-169.

[14] Shyi-Tsong Wu and Bin-Chang Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards," *Computers & Security* 22, no. 6 (2003): 547-550.

[15] Wu and Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards."

[16] Hwang and Li, "A New Remote User Authentication Scheme Using Smart Cards."

[17] Chien, Jan, and Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card."

[18] Hwang, Lee, and Tang, "A Simple Remote User Authentication Scheme."

[19] Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards."

[20] Shafi Goldwasser, "The Search for Provably Secure Cryptosystems," in *Cryptology and Computational Number Theory, Proceedings of Symposia in Applied Mathematics* 42, ed. C. Pomerance (Washington: American Mathematical Society, 1990), 89-113.

[21] Hwang and Li, "A New Remote User Authentication Scheme Using Smart Cards."

[22] Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards."

[23] Wu and Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards."

[24] Tang, Lee, and Hwang, "A Simple Remote User Authentication Scheme."

[25] Chien, Jan, and Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card."

TZUNG-HER CHEN was born in Tainan, Taiwan, Republic of China, in 1967. He received his B.S. degree from the National Taiwan Normal University (Department of Information & Computer Education) in 1991 and his M.S. degree from Feng Chia University (Department of Information Engineering), in 2001. In 2005, he obtained his Ph.D. degree from the National Chung Hsing University (Department of Computer Science). He has been Assistant Professor in the Department of Computer Science and Information Engineering at the National Chiayi University since August 2005. His research interests include information hiding, multimedia security, digital rights management, and network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society. *Address for Correspondence*: Department of Computer Science and Information Engineering, National Chiayi University, 300 University Road, Chia-Yi City, Taiwan 600, R.O.C.; *Fax*: 886-5-2717741; *E-mail*: thchen@mail.ncyu.edu.tw.

GWOBOA HORNG received his B.S. degree in Electrical Engineering from National Taiwan University in 1981 and his M.S. and Ph.D. degrees from University of Southern California in 1987 and 1992 respectively, all in Computer Science. Since 1992, he has been on the faculty of the Institute of Computer Science at National Chung-Hsing University, Taichung, Taiwan, R.O.C. His current research interests include artificial intelligence, cryptography and information security. *Address for Correspondence*: Department of Computer Science, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung, Taiwan 402, R.O.C.

DU-SHIAU TSAI received his B.S. degree from the Providence University (Department of Computer Science and Information Management), Taiwan, in 1996 and his M.S. degree from the National Chung-Hsing University (Institute of Computer Science), Taiwan, in 2003. He is currently pursuing his Ph.D. degree in the Institute of Computer Science, National Chung-Hsing University. His research interests include cryptography, information security and digital watermarking. *Address for Correspondence*: Department of Computer Science, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung, Taiwan 402, R.O.C. and Department of Information Management, Hsiuping Institute of Technology, 11, Gongye Rd., Dali City, Taichung County, Taiwan 412, R.O.C.