Computers & Security (2005) **24**, 50–56

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

An improvement of Hwang–Lee–Tang's simple remote user authentication scheme

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

Department of Computer Engineering, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea

Received 31 March 2004; revised 31 March 2004; accepted 2 June 2004
Available online 28 January 2005

KEYWORDS
Cryptography;
Authentication;
Security;
Smart card;
Hash function

Abstract Recently, Hwang–Lee–Tang proposed a simple remote user authentication scheme using smart card, whereby it does not require any password or verification tables in the remote system and any legal users could choose and change their passwords freely. However, their schemes previously generated user's secret hash values are insecure if the secret key of the server is leaked or is stolen, also when the smart card is stolen, unauthorized users can easily change new password of the smart card. Furthermore, their scheme cannot resist the denial of service attack using stolen smart card and does not provide mutual authentication. Accordingly, the current paper demonstrates the vulnerability of Hwang–Lee–Tang's scheme and presents an enhancement to resolve such problems. As a result, the proposed scheme previously generated secret hash values are secure even if the secret key of the system is leaked or is stolen and enables users to update their passwords freely and securely, while also providing mutual authentication and fast detect it when user inputs wrong password. In addition, the computational costs of this scheme are less than those of any previously proposed schemes.

Introduction

User authentication is an important part of security, along with confidentiality and integrity, for systems that allow remote access over untrustworthy networks, like the Internet. As such, a remote password authentication scheme (Lamport, 1981; Chang and Wu, 1991; Wu and Sung, 1996; Jan and Chen, 1998; Tan and Zhu, 1999; Yang and Shieh, 1999; Aoskan et al., 1999) authenticates the legitimacy of users over an insecure channel, where the password is often regarded as a secret shared between the remote system and the user. Based on knowledge of the password, the user can use it to create and send a valid login message to a remote system to gain the right to access.

* Corresponding author. Tel.: 82 53 950 5553; fax: 82 539574846.
E-mail address: yook@knu.ac.kr (K.-Y. Yoo).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.06.004

Meanwhile, the remote system also uses the shared password to check the validity of the login message and authenticate the user.

In 1981, Lamport proposed a remote password authentication scheme using a password table to achieve user authentication. However, one of the weaknesses of Lamport's scheme is that a verification table should be stored in the remote system in order to verify the legitimacy of a user. If an intruder can somehow break into the server, the contents of the verification table can be easily modified. Thus, recently, many password authentication schemes (Chang and Wu, 1991; Wu, 1995; Yang and Shieh, 1999; Hwang and Li, 2000; Sun, 2000; Chien et al., 2002; Hwang et al., 2002; Wu and Chieu, 2003) have recognized this problem and proposed solutions using smart cards in which the verification table is no longer required in the remote system. In 2000, Hwang and Li pointed out that Lamport's scheme (Lamport, 1981) suffers from the risk of a modified password table and the cost of protecting and maintaining the password table. Therefore, they proposed a new user authentication scheme using smart cards to eliminate the risk and cost. Hwang and Li's scheme can withstand replaying attacks and also authenticate users without maintaining a password table. Later, Sun (2000) proposed an efficient smart card-based user authentication scheme to improve the efficiency of Hwang and Li's scheme (Hwang and Li, 2000), and more recently, Hwang—Lee—Tang (Hwang et al., 2002) proposed a simple remote user authentication scheme, whereby it does not require any password or verification tables in the remote system and any legal users could choose and change their passwords freely without the help of a remote system. They claimed that their scheme provided effective authentication and also requires much fewer computations than other schemes as in Wu (1995), Jan and Chen (1998), Yang and Shieh (1999), Hwang and Li (2000) and Chien et al. (2002).

However, their schemes previously generated user's secret hash values are insecure if the secret key of the server is leaked or is stolen, also when the smart card is stolen, unauthorized users can easily change new password of the smart card. Furthermore, their scheme cannot resist the denial of service attack using stolen smart card and does not provide mutual authentication. In some situations, mutual authentication is necessary to provide higher security. Accordingly, the current paper demonstrates the vulnerability of Hwang—Lee—Tang's scheme to above mentioned attacks and presents an enhancement to resolve such problems. As a result, the proposed scheme previously generated secret hash values are secure even if the secret key of the system is leaked or is stolen and enables users to update their passwords freely and securely, while also providing mutual authentication and fast detect it when user inputs wrong password. In addition, the computational costs of this scheme are less than those of any previously proposed schemes.

The remainder of this paper is organized as follows: next section briefly reviews Hwang—Lee—Tang's scheme, then follows its weaknesses. Further the proposed scheme is presented, while in the following sections the security and efficiency of the proposed scheme are discussed. Some final conclusions are given in last section.

Hwang—Lee—Tang's scheme

This section briefly reviews Hwang—Lee—Tang's scheme, which has a registration, login, authentication phase and password change phase, as explained in the following:

Registration phase: The user U_i chooses a password PW_i, and then computes $h(PW_i)$, where $h(\ )$ is a collision resistant one-way hash function. The user U_i submits their identifier ID_i and $h(PW_i)$ to the remote system. These private data must be sent in person or over a secure channel. Upon receiving the registration request, the system performs the following steps:

1. Compute $A_i = h(ID_i \oplus x) \oplus h(PW_i)$, where x is a secret key maintained by the system.
2. The system then personalizes the smart card with the secure information: $\{ID_i, A_i, h(\ )\}$.

Login phase: Fig. 1 illustrates the login and authentication phases in Hwang—Lee—Tang's scheme. If the user U_i wants to login, they attach their smart card to the card reader and key in their identifier ID_i and password PW_i^*, then the smart card performs the following operations:

1. Compute the following two integers: $B_i = A_i \oplus h(PW_i^*)$ and $C_1 = h(B_i \oplus T)$, where T is the current date and time of the input device.
2. Send a message $m = \{ID_i, C_1, T\}$ to the remote system.

Authentication phase: Upon receiving message m at time T', the remote system authenticates the user based on the following steps:

1. Verify the format of ID_i. If the format is incorrect, the system rejects the login request.

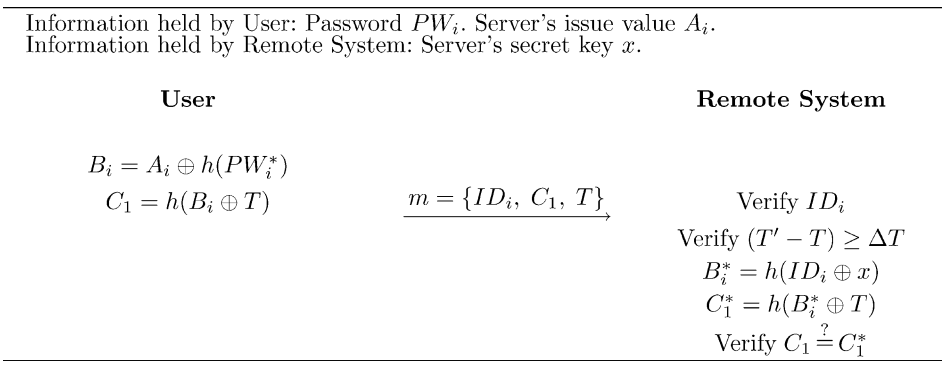

Figure 1 Login and authentication phases in Hwang—Lee—Tang's scheme.

2. Verify the validity of the time interval between T and T'. If $(T^{'} - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for a transmission delay, the remote system rejects the login request.
3. The system computes the following two integers: $B_i^* = h(\mathrm{ID}_i \oplus x)$ and $C_1^* = h(B_i^* \oplus T)$, and compares C_1 and C_1^*. If they are equal, then the system accepts the login request, otherwise it rejects the login request.

Password change phase: According to Hwang—Lee—Tang's scheme, when an authorized user U_i wants to change their password, they have to perform the following procedures:

1. Compute $B_i = A_i \oplus h(\mathrm{PW}_i^*) = h(\mathrm{ID}_i \oplus x)$.
2. Select new password $\mathrm{PW}_i^{'}$ and compute $h(\mathrm{PW}_i^{'})$.
3. Compute $A_i^{'} = B_i \oplus h(\mathrm{PW}_i^{'})$.
4. Store $A_i^{'}$ in smart card in place of A_i.

Cryptanalysis on Hwang—Lee—Tang's scheme

Hwang—Lee—Tang's scheme has the following security flaws:

1. Suppose intruder has stolen the remote systems secret key x. It is obvious that he can compute each user's secret hash value as $B_i = h(\mathrm{ID}_i, x)$ in Hwang—Lee—Tang's scheme. The corrupted key may be changed to stop intruder's activity by choosing a new and fresh secret key. However, it would be much expensive to recompute all secret hash values at a time and communicate to the users.
2. When the smart card is stolen, unauthorized users can easily change new password of the card in password change phase as following:
   (a) The smart card computes $B_i = A_i \oplus h(\mathrm{PW}_a^*) = h(\mathrm{ID}_i \oplus x) \oplus h(\mathrm{PW}_i) \oplus h(\mathrm{PW}_a^*)$, where $h(\mathrm{PW}_a^*)$ is unauthorized user's arbitrary password.
   (b) Unauthorized user select arbitrary new password $\mathrm{PW}_a^{'}$ and then smart card computes $h(\mathrm{PW}_a^{'})$.
   (c) The smart card computes $A_i^{'} = B_i \oplus h(\mathrm{PW}_a^{'})$.
   (d) Store $A_i^{'}$ in smart card in place of A_i without any checking.
3. If malicious user stole the user U_i's smart card for a short time and change arbitrary new password like above mentioned (1), then the legal user U_i's succeeding login requests will be denied unless he re-registers to remote system again because $C_1 \neq C_1^*$ in authentication phase. Therefore, Hwang—Lee—Tang's scheme is vulnerable to the denial of service attack using stolen smart card.
4. If user U_i inputs wrong password by mistake, this wrong password will be detected by remote system in authentication phase. Therefore, Hwang—Lee—Tang's scheme is slow to detect the user's wrong password.

Proposed scheme

This section proposes an enhancement to Hwang—Lee—Tang's scheme that can withstand the security flaws described in previous sections. In addition, the proposed scheme also allows users to update their passwords freely and securely without the help of a remote system and provides mutual authentication between the user and a remote system. The security of the proposed scheme is based on a one-way hash function, and consists of a registration, login, authentication phase and password change phase.

Registration phase: Fig. 2 illustrates the registration phase in proposed scheme. Like Hwang—Lee—Tang's scheme, let x be a secret key

User		Remote System
Select ID_i, PW_i	$\xrightarrow{\{ID_i,\ PW_i\}}$	$V_i = h(ID_i, T_{TSA}, x)$ $A_i = h(ID_i, T_{TSA}, x) \oplus PW_i$
	$\xleftarrow{\{ID_i,\ V_i,\ A_i,\ h(\cdot)\}}$	

Figure 2 Registration phase in proposed scheme.

maintained by the system. The user U_i submits their identifier ID_i and chosen password PW_i to the system. These private data must be sent in person or over a secure channel. Upon receiving the registration request, the system performs the following steps:

1. Computes $V_i = h(ID_i, T_{TSA}, x)$ and $A_i = h(ID_i, T_{TSA}, x) \oplus PW_i$, where x is a secret key maintained by the system, TSA is a trusted time stamping authority that provides current time stamp whenever required, T_{TSA} is time stamp provided by TSA and $h(\ )$ is a collision resistant one-way hash function.
2. The system then personalizes the smart card with the secure information: $\{ID_i, V_i, A_i, h(\ )\}$.

Login phase: Fig. 3 illustrates the login and authentication phases in proposed scheme. If the user U_i wants to login, they attach their smart card to the card reader and key in their identifier ID_i and password PW_i^*, then the smart card performs the following operations:

1. Computes $B_i = A_i \oplus PW_i^*$, and verifies whether B_i equals the stored V_i. If they are equal, then computes $C_1 = h(B_i, T)$, where T is the current date and time of the input device.
2. Send a message $m = \{ID_i, C_1, T\}$ to the remote system.

Authentication phase: Upon receiving the authentication request message $m = \{ID_i, C_1, T\}$, the remote system and smart card execute the following steps for mutual authentication between the user U_i and the remote system.

1. The system verifies the format of ID_i. If the format is incorrect, the system rejects the login request.
2. The system verifies the validity of the time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for a transmission delay, the remote system rejects the login request.
3. The system computes the following two integers: $B_i^* = h(ID_i, T_{TSA}, x)$ and $C_1^* = h(B_i^*, T)$, and compares C_1 and C_1^*. If they are equal, then the system accepts the login request and proceeds to Step 4, otherwise it rejects the login request.

Information held by User: Password PW_i. Server's issue value V_i, A_i.
Information held by Remote System: Server's secret key x, T_{TSA}.

User		Remote System
$B_i = A_i \oplus PW_i^* = h(ID_i, T_{TSA}, x)$ Verify $B_i \stackrel{?}{=}$ stored V_i $C_1 = h(B_i, T)$	$\xrightarrow{m = \{ID_i,\ C_1,\ T\}}$	Verify ID_i Verify $(T' - T) \geq \Delta T$ $B_i^* = h(ID_i, T_{TSA}, x)$ $C_1^* = h(B_i^*, T)$ Verify $C_1 \stackrel{?}{=} C_1^*$
Verify $(T''' - T'') \geq \Delta T$ $C_2^* = h(B_i, C_1, T'')$ Verify $C_2 \stackrel{?}{=} C_2^*$	$\xleftarrow{\{C_2,\ T''\}}$	$C_2 = h(B_i^*, C_1^*, T'')$

Figure 3 Login and authentication phases in proposed scheme.

4. The system acquires the current time stamp T'' and computes $C_2 = h(B_i^*, C_1^*, T'')$. The system sends back the message $\{C_2, T''\}$.
5. Upon receiving the message $\{C_2, T''\}$, the user U_i verifies the validity of the time interval between T'' and T''', then computes $C_2^* = h(B_i, C_1, T'')$ and compares C_2 and C_2^*. If they are equal, the user U_i believes that the responding part is the real system and the mutual authentication is complete, otherwise the user U_i interrupts the connection.

Password change phase: If the user U_i wants to change their old password PW_i to a new password PW_i', they only need to perform the procedures given below, without any help from the remote system:

1. Compute $B_i = A_i \oplus PW_i^* = h(ID_i, T_{TSA}, x)$.
2. Compare B_i and store V_i in smart card.
3. If they are equal, then the user U_i selects new password PW_i', otherwise it rejects the password change request.
4. Compute $A_i' = B_i \oplus PW_i'$.
5. Store A_i' in smart card in place of A_i.

Security analysis

In this section, we examine the security of our proposed scheme:

1. Due to the fact that a one-way hash function is computationally difficult to invert, it is extremely difficult for any attacker to derive the system secret key x from $B_i = h(ID_i, T_{TSA}, x)$. Even if the smart card of the user U_i is picked up by an attacker, it is still difficult for the attacker to derive x.
2. If an attacker tries to forge a valid parameter C_1, they must have the system secret information x, because C_1 must be derived from PW_i and A_i. However, this is infeasible, as A_i has to be obtained from the system secret information x.
3. For replay attacks, neither the replay of an old login message $\{ID_i, C_1, T\}$ in the login phase nor the replay of the remote system's response message in Step 4 of the authentication phase will work, as it will fail in Steps 2 and 5 of the authentication phase due to the time interval $(T' - T) \geq \Delta T$ and $(T''' - T'') \geq \Delta T$, respectively.
4. Given a valid request message $m = \{ID_i, C_1, T\}$, it is infeasible that an attacker can compute B_i using equation $C_1 = h(B_i, T)$, because it is a one-way property of a secure one-way hash function.
5. The proposed scheme can resist an impersonation attack. An attacker can attempt to modify a message $\{ID_i, C_1, T\}$ into $\{ID_i, C_A, T_A\}$, where T_A is the attacker's current date and time, so as to succeed in Step 2 of the authentication phase. However, such a modification will fail in Step 3 of the authentication phase, because an attacker has no way of obtaining the value $B_i = h(ID_i, T_{TSA,x})$ to compute the valid parameter C_1.
6. If a masqueraded server tries to cheat the requesting user U_i, it has to prepare a valid message $\{C_2, T''\}$. However, this is infeasible, as there is no way to derive the value B_i^* to compute the value $C_2 = h(B_i^*, C_1^*, T'')$, due to the one-way property of the secure one-way hash function. Plus, a replay message can be exposed because of the time stamp.
7. Because of smart card verify B_i using stored V_i in Step 2 of the password change phase, when the smart card is stolen, unauthorized users cannot change new password of the card. Thus, proposed scheme can resist the denial of service attack using stolen smart card.
8. Several server spoofing attacks have been recently proposed (Aoskan et al., 1999). The attacker can manipulate the sensitive data of legitimate users via setting up fake servers. Therefore, a secure remote user authentication scheme with smart card must have the ability to work against such attacks. Proposed scheme provides mutual authentication to withstand the server spoofing attack.
9. Let the secret key x be revealed by some accident and it comes into knowledge of the remote system. Now he can reinitialize the secret key x as new system parameter. With the revealed key any attacker can try to obtain the secret hash value $h(ID_i, T_{TSA}, x)$ of previously registered ID_i or that may try to obtain

Table 1 Comparison of security properties

	Hwang—Lee—Tang's scheme	Proposed scheme
Denial of service attack using stolen smart card	Yes	No
Secret key forward secrecy	No	Yes
Change password phase	Insecure	Secure
Wrong password detection	Slow	Fast
Mutual authentication	Not supported	Supported

Table 2 Comparisons of computation costs

	Hwang–Lee–Tang's scheme		Proposed scheme	
	User	Server	User	Server
Registration phase	$1T(h)$	$1T(h)$	No	$1T(h)$
Login and authentication phase for unilateral authentication	$2T(h)$	$2T(h)$	$1T(h)$	$2T(h)$
Login and authentication phase for mutual authentication	Not supported	Not supported	$1T(h)$	$1T(h)$
Change password phase	$2T(h)$		No	

$T()$:computation time; h: secure one-way hash operation.

a fake postdated secret hash value. When he goes to obtain some previous secret hash value, he is required to compute $h(\mathrm{ID}_i, T_{\mathrm{TSA}}, x)$, where T_{TSA} is postdated timestamp that prevents him to compute $h(\mathrm{ID}_i, T_{\mathrm{TSA}}, x)$. And for the same reason he cannot generate fake postdated secret hash value for some new ID.

The security properties of Hwang–Lee–Tang's scheme and the proposed scheme are summarized in Table 1. In contrast to Hwang–Lee–Tang's scheme, the proposed scheme is more secure.

Comparisons of computation costs

The computation costs of Hwang–Lee–Tang's scheme and the proposed scheme in registration, login, authentication, and change password phases are summarized in Table 2. In registration, login, authentication, and change password phases, Hwang–Lee–Tang's scheme requires totally 8 times hash operations for unilateral authentication, but proposed scheme requires totally 4 times hash operations. For mutual authentication, proposed scheme requires 6 times hash operations. It is obvious that our scheme is more efficient than Hwang–Lee–Tang's scheme. However, proposed scheme provides mutual authentication between the user and a remote system.

Conclusion

In the current paper, an enhancement to Hwang–Lee–Tang's scheme was proposed. Besides, the proposed scheme achieves the same advantages as Hwang–Lee–Tang's scheme and has the following merits:

1. Any legal users can select and change their password freely and securely.
2. The denial of service attack using stolen smart card is completely solved.
3. Previously generated secret hash values are secure even if the secret key of the system is leaked or is stolen.
4. The server spoofing attack is completely solved by providing mutual authentication.
5. User's wrong input password is detected fast.
6. The computational costs are less than those of any previously proposed schemes.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments. This work was supported by the Brain Korea 21 Project in 2004.

References

Aoskan N, Debar H, Steiner M, Waidner M. Authentication public terminals. Comput Netw 1999;31:861–970.

Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proc-E 1991;138(3):165–8.

Chien HY, Jan JK, Tseng YM. An efficient and practical solution to remote authentication: smart card. Comput Secur 2002; 21(4):372–5.

Hwang MS, Li LH. A new remote user authentication scheme using smart cards. IEEE Trans Consum Electron February 2000;46(1).

Hwang MS, Lee CC, Tang YL. A simple remote user authentication. Math Comput Model 2002;36:103–7.

Jan JK, Chen YY. 'Paramita wisdom' password authentication scheme without verification tables. J Syst Softw 1998;42: 45–57.

Lamport L. Password authentication with insecure communication. Commun ACM 1981;24(11):770–2.

Sun HM. An efficient remote user authentication scheme using smart cards. IEEE Trans Consum Electron November 2000; 46(4).

Tan K, Zhu H. Remote password authentication scheme based on cross-product. Comput Commun 1999;18:390–3.

Wu TC. Remote login authentication scheme based on a geometric approach. Comput Commun 1995;18(12):959–63.
Wu ST, Chieu BC. A user friendly remote authentication scheme with smart cards. Comput Secur 2003;22(6):547–50.
Wu TC, Sung HS. Authentication passwords over an insecure channel. Comput Secur 1996;15(5):431–9.
Yang WH, Shieh SP. Password authentication schemes with smart card. Comput Secur 1999;18(8):727–33.

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 PhD degree in the Kyungpook National University. His research interests include cryptography and network security.

Eun-Kyung Ryu received her MS in the Information & Communication Engineering from Keimyong University, South Korea. She is now working toward the PhD 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 PhD 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.