An Improved Hwang-Lee-Tang Remote User Authentication Scheme

Sheikh Ziauddin
Department of Computer Science
COMSATS Institute of Information Technology, Islamabad, Pakistan
email:sh.ziauddin@gmail.com

Abstract: In this paper, we present a secure and efficient remote authentication scheme by improving Hwang-Lee-Tang's scheme. The security of our scheme is based on the onewayness and collision-resistance properties of the hash functions being used. The proposed scheme is able to withstand all commonly known attacks against remote authentication schemes. In addition, the scheme does not store a password table on the server, provides mutual authentication between the user and the server, does not reveal user's password to the server, allows the user to freely choose a password of her choice, and allows the user to change her password by running a simple protocol with the server.

1 Introduction

The classic technique for remote authentication is based on users' passwords. With the passage of time, it has been realized that the use of password alone is not enough from the security point of view because the typical human-selected passwords have low entropy. Therefore, in modern times, many attempts have been made to build two-factor secure remote authentication systems by combining the passwords and the smart cards [CW93, CH93, HL00, Sun00, LHY02, HLT02, CJT02, SLH03a, AL03, CLH04, LKY04, YRY05, LC05].

Lamport [Lam81] was the first one to propose a remote user authentication scheme. In his scheme, a table of passwords is maintained on the server for users' verification. The major drawback of his scheme is that if the server is compromised, the secret passwords of all the users are disclosed. Subsequently, many password authentication schemes have been presented that do not rely on verification tables stored on the server. Sun [Sun00] presented a two-factor authentication scheme using a password and a smart card. Unfortunately, their scheme provides only uni-directional authentication from the user to the server. In addition, the user's password is known to the server and the scheme does not allow the user to change her password. Hwang, Lee, and Tang [HLT02] presented a scheme that allows for user's password change but no verification check is conducted before committing the password change. Chien et al. [CJT02] proposed another password authentication scheme using hash functions. Their scheme also suffers from the problems of password being known to the server and having no password change option. Lee et al. [LKY04] and

Yoon et al. [YRY05] later presented their respective schemes but they also suffer from the problem of user's password revealed to the server. In addition, in [LKY04], no verification check is performed before password change and in [YRY05], it is easy to retrieve the password if the smart card is stolen.

In addition to the above hash function-based schemes, another research direction is to use public key cryptography for remote authentication [YS99, FLZ02, SLH03b, SLH03a, HL00, AL03]. The main disadvantage of public key schemes is their high computational cost which makes them unsuitable for many practical applications.

In this paper, we present a remote authentication scheme which is constructed from hash functions (e.g., SHA-256). At registration time, the user sends hash of her password to the server and receives a smart card containing some information generated from a combination of the user's password and the server's secret key. At authentication time, the user uses her password and smart card to generate user-to-server messages while the server uses its secret key to generate server-to-user messages. If the messages are successfully validated by the receiving entities, mutual authentication is carried out between the user and the server.

The rest of the paper is organized as follows. In Section 2, we present the assumptions and the threat model for the scheme. Section 3 describes Hwang et al.'s scheme and its weaknesses. In Section 4, we describe the working of the proposed scheme. The security of our scheme is analyzed in Section 5, and finally, we conclude the paper in Section 6.

2 Adversarial Model

In this section, we outline the assumptions made about the proposed scheme and describe the capabilities of the adversary against the scheme. Major points of our model are as follows.

- The user and the server participate honestly in the protocol.
- The adversary cannot steal the server's secret.
- The adversary can steal either the user's password or the smart card, but not both.
- The user and the server use synchronized clocks or they have access to a common trusted time server to get the current time.
- A secure and authenticated channel exists between the communicating parties during the registration phase.
- During authentication and password change phases, the communication takes place in a completely adversarially controlled channel.
- The smart card is tamper resistant. The data can be overwritten but only through a provided interface, e.g., the one used in the password change phase of the proposed scheme.

- Once a smart card is stolen, all the stored information can be extracted by the adversary, e.g., by using reverse engineering techniques.

3 Hwang-Lee-Tang's Scheme

Notation

First we describe the notation that we will use in this paper to denote the elements of both Hwang et al.'s scheme and the proposed scheme. We use ID to denote the identity of the user in a format suitable for the specific application. PW and k denote the user's password and the server's secret key, respectively. We use SC to denote the smart card issued by the server to the user. $\oplus$ denotes an exclusive-or operation. We use $\mathsf{h}(\cdot)$ to denote description of the cryptographically secure hash function being used in the protocol. T, T_1, T_1', T_2, T_2' represent timestamps at different times and Δt denotes the maximum allowed network delay time for a single message passed between the user and the server. PCR denotes a special message in a specific format which we name *password change request*. This message is part of the communication during password change phase only and serves to differentiate between the authentication requests and the password change requests.

3.1 Description of Hwang-Lee-Tang's Scheme

Our scheme is based on Hwang-Lee-Tang [HLT02] scheme. In this section, we briefly describe their scheme and point out its weaknesses. The scheme has three phases: registration, authentication, and password change.

3.1.1 Registration Phase

The user sends the hash of her password $\mathsf{h}(PW)$ and her ID to the server. The server receives the message, calculates $A = \mathsf{h}(ID \oplus k) \oplus \mathsf{h}(PW)$, and personalizes a smart card to the user containing the values $\mathsf{h}(\cdot), ID,$ and A.

3.1.2 Authentication Phase

The user (smart card) calculates $B = A \oplus \mathsf{h}(PW)$ using her password PW and the value A stored on the smart card, gets the current timestamp T, calculates $C = \mathsf{h}(B \oplus T)$, and sends (ID, C, T) to the server. After receiving the message, the server verifies the format of ID and the validity of T. It then calculates $B' = \mathsf{h}(ID \oplus k)$ and $C' = \mathsf{h}(B' \oplus T)$, and verifies that $C \stackrel{?}{=} C'$. If the verification is successful, the user's authentication request is accepted.

3.1.3 Password Change Phase

The user (smart card) calculates $B = A \oplus \mathsf{h}(PW)$ using her old password PW. She next calculates $A' = B \oplus \mathsf{h}(PW')$ using her new password PW'. Stored A on the smart card is then replaced with A'.

3.2 Weaknesses

One weakness of the scheme is its insecure password change phase. Consider an adversary who steals the smart card of a user. The adversary gives any arbitrary password PW' and calculates $B = A \oplus \mathsf{h}(PW')$. The adversary then selects a new password PW'' and calculates $A' = B \oplus \mathsf{h}(PW'')$. Next, stored A on the smart card is replaced with A' without any verification. This shows that it is easy for an adversary to change the password of any user without knowing the original password. Using this new password, the adversary can impersonate the user in the protocol as he possesses both the secrets now.

Another necessary security requirement missing in their scheme is the ability to provide mutual authentication. Mutual authentication is necessary in most remote authentication systems such as those used for electronic commerce where the users want to make sure that they are communicating with the legitimate server before committing any financial transaction.

In next section, we present our scheme which removes the above-mentioned flaws from their scheme. In addition, our scheme provides many other desirable features.

4 Proposed Scheme

4.1 Registration Phase

The registration phase of our scheme is the same as that of Hwang-Lee-Tang's scheme. During this phase, the following steps are carried out.

1. The user freely selects a password PW of her choice along with an arbitrary unique ID and sends her ID along with the hash of her password $\mathsf{h}(PW)$ to the server.
2. After receiving the user's message, the server calculates $A = \mathsf{h}(ID \oplus k) \oplus \mathsf{h}(PW)$ and issues a smart card to the user that contains the values $\mathsf{h}(\cdot), ID,$ and A.

Figure 1 schematically describes the registration phase of the proposed scheme.

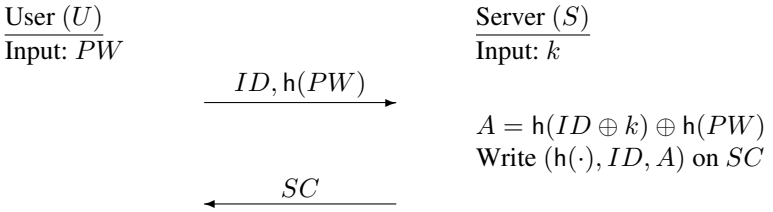

Figure 1: Registration phase of the proposed scheme (Same as that of Hwang-Lee-Tang)

4.2 Authentication Phase

During this phase, the user inserts her smart card in a card reader, keys in her password on a terminal, and then the user (the smart card) and the server communicate with each other for some time. At the end of a successful communication, they authenticate each other. The user's secrets are her password PW and the smart card while the server is in possession of its secret key k. During this phase, the following steps are carried out.

1. The user calculates a hash of her password $\mathsf{h}(PW)$, reads the value A from the smart card, and XORs them to get a value B. Next, she gets the current timestamp T_1, calculates $C_1 = \mathsf{h}(B \oplus T_1)$ and sends C_1, T_1 along with her ID to the server.

2. After receiving the user message, the server verifies the format of user's ID. Next, the server gets the current timestamp T_1' and verifies that $T_1' - T_1$ does not exceed ΔT. It next calculates $B' = \mathsf{h}(ID \oplus k)$ and $C_1' = \mathsf{h}(B' \oplus T_1)$ and verifies that C_1 and C_1' are equal. If any of the verifications described above fail, the request is rejected. Otherwise the request is accepted, i.e., the user is successfully authenticated. Next, the server gets the current timestamp T_2, calculates $C_2 = \mathsf{h}(B' \oplus T_2)$ and sends C_2 and T_2 to the user.

3. After receiving the server message, the user gets the current timestamp T_2' and verifies that $T_2' - T_2$ does not exceed ΔT. The user calculates $C_2' = \mathsf{h}(B \oplus T_2)$ and verifies that C_2 and C_2' are equal. If any of the verifications described above fail, the request is rejected. Otherwise the request is accepted, i.e., the server is successfully authenticated.

If both steps 2 and 3 are successful, this indicates a successful mutual authentication being carried out. Figure 2 schematically describes the authentication phase of the proposed scheme.

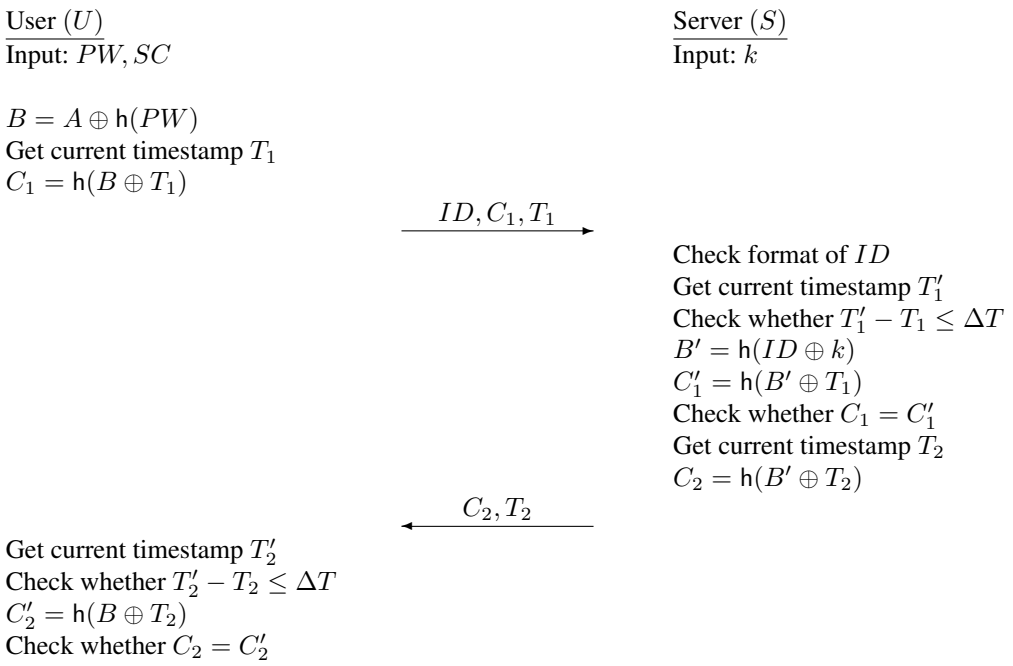

Figure 2: Authentication phase of the proposed scheme

4.3 Password Change Phase

Similar to authentication phase, the user inserts her smart card in a card reader, keys in her password on a terminal, and then the user (the smart card) and the server communicate with each other for some time. At the end of a successful communication, the user changes her password. The user's secrets are her existing password PW and SC while the server has its secret k. During this phase, the following steps are carried out.

1. The user calculates a hash of her password $\mathsf{h}(PW)$, reads the value A from the smart card, and XORs them to get a value B. She gets the current timestamp T_1, calculates $C_1 = \mathsf{h}(B \oplus T_1 \oplus PCR)$ and sends C_1, T_1 and PCR along with her ID to the server.

2. After receiving the user message, the server verifies the formats of ID and PCR. It gets the current timestamp T_1' and verifies that $T_1' - T_1$ does not exceed ΔT. The server next calculates $B' = \mathsf{h}(ID \oplus k)$ and $C_1' = \mathsf{h}(B' \oplus T_1 \oplus PCR)$ and verifies that C_1 and C_1' are equal. If any of the above verifications fail, the password change request is rejected. Otherwise, the request is accepted and the server gets the current timestamp T_2, calculates $C_2 = \mathsf{h}(B' \oplus T_2 \oplus PCR)$ and sends C_2 and T_2 to the user.

3. After receiving the server message, the user gets the current timestamp T_2' and veri-

fies that $T_2' - T_2$ does not exceed ΔT. She next calculates $C_2' = \mathsf{h}(B \oplus T_2 \oplus PCR)$ and verifies that C_2 and C_2' are equal. If any of the above verifications fail, the request is rejected. Otherwise the user calculates $A' = B \oplus \mathsf{h}(PW')$ where PW' is the new password of the user and the value A on smart card is replaced with A'.

Figure 3 schematically describes the password change phase of the proposed scheme.

User (U)		Server (S)
Input: PW, SC		Input: k
$B = A \oplus \mathsf{h}(PW)$		
Get current timestamp T_1		
$C_1 = \mathsf{h}(B \oplus T_1 \oplus PCR)$		
	$\xrightarrow{ID, C_1, T_1, PCR}$	
		Check format of ID
		Check format of PCR
		Get current timestamp T_1'
		Check whether $T_1' - T_1 \leq \Delta T$
		$B' = \mathsf{h}(ID \oplus k)$
		$C_1' = \mathsf{h}(B' \oplus T_1 \oplus PCR)$
		Check whether $C_1 = C_1'$
		Get current timestamp T_2
		$C_2 = \mathsf{h}(B' \oplus T_2 \oplus PCR)$
	$\xleftarrow{C_2, T_2, PCR}$	
Get current timestamp T_2'		
Check whether $T_2' - T_2 \leq \Delta T$		
$C_2' = \mathsf{h}(B \oplus T_2 \oplus PCR)$		
Check whether $C_2 = C_2'$		
$A' = B \oplus \mathsf{h}(PW')$		
Replace A on SC with A'		

Figure 3: Password change phase of the proposed scheme

5 Security Analysis

In absence of a common set of necessary and sufficient security requirements for smart card-based password authentication schemes, we analyze the security of our scheme against an extensive set of security requirements that we consider to be necessary for a two-factor remote authentication scheme.

Replay attack. This attack is not feasible against our scheme. To see this, consider an adversary trying to replay a message (ID, C_1, T_1) sent from the client to the server during

the authentication phase. Clearly, this attack will be detected in Step 2 by the server. Also note that the adversary cannot replace T_1 by a newer time because he cannot generate a valid C_1 for that time without stealing the smart card and knowing the password. Further note that it is highly unlikely for the adversary to get the same C_1 for time $\hat{T} \neq T_1$ due to collision-resistance property of the hash function. The same logic applies for replaying a message from the server to the client.

User impersonation. To impersonate a user, the adversary has to fabricate a valid message (ID, C_1, T_1). As mentioned above, it is not feasible to find C_1 without stealing both the password and the smart card. Also it is not feasible to recover the password (or the value A) from C_1 due to onewayness of hash function.

Server impersonation/Server spoofing. To impersonate the server, the adversary has to fabricate a valid message (C_2, T_2). It is not feasible to find C_2 without stealing the server's secret k. Also it is not feasible to recover k from C_2 due to onewayness of hash function.

Stolen verifier attack. This attack is not possible against our system as the server does not maintain any verification table for users' passwords. Instead, the data needed for verification is stored on the users' smart cards.

Password guessing attack. The password guessing attack is not feasible against our scheme. To see this, first note that the hash of the password is never transmitted over the channel. Next, consider an adversary which intercepts and stores a message (ID, C_1, T_1). There is no way for the adversary to verify the correctness of his password guesses because the value C_1 is a function of not only the password but also of the value A stored on the smart card. This makes it impossible to verify the correctness of a guess without stealing the smart card as well. We point out that password guessing using a compromised smart card is not a valid attack because, in two-factor schemes (using passwords and smart cards), there is no way to stop an adversary from carrying out such an attack. The attack can be countered by replacing low entropy passwords with high entropy secrets such as passphrases or biometrics. Note that this change does not make the above attack unsuccessful, rather it only increases the time complexity of the attack.

Stolen smart card attack. The only secret stored on the smart card is $A = \mathsf{h}(ID \oplus k) \oplus \mathsf{h}(PW)$. Clearly it is not feasible to find either PW or k from A without breaking the onewayness of the cryptographic hash function involved. Also note that the adversary can neither fabricate (ID, C_1, T_1) nor (C_2, T_2) without knowing either the user's password or the server's secret in addition to the smart card data.

Stolen password attack. Stealing the password will not help the adversary. To fabricate a message (ID, C_1, T_1), the adversary has to find $B = A \oplus \mathsf{h}(PW)$. As the adversary already knows $\mathsf{h}(PW)$, clearly the entropy of B is equal to the entropy of A . As A is generated by applying a hash function on the server secret k, it is neither feasible to predict k due to its high entropy, nor it is feasible to find a $\hat{k} \neq k$ such that $A = \mathsf{h}(ID \oplus \hat{k})$ due to the collision-resistance of the hash function.

6 Conclusions

In this paper, we presented a remote mutual authentication scheme. We used cryptographic hash functions as building blocks of our scheme. We presented a thorough security analysis and showed that the proposed scheme is able to withstand many attacks against remote authentication schemes. The proposed scheme does not store a password table on the server, provides mutual authentication and allows the user to easily change her password. The scheme is also efficient as it uses just a few hash operations only.

References

[AL03] A. K. Awasthi and S. Lal. A remote user authentication scheme using smart cards with forward secrecy. *IEEE Transactions on Consumer Electronics*, 49(4):1246–1248, 2003.

[CH93] C. Chang and S. Hwang. Using smart cards to authenticate remote passwords. *Computers and Mathematics with Applications*, 26(7):19–27, 1993.

[CJT02] H. Chien, J. Jan, and Y. Tseng. An efficient and practical solution to remote authentication: Smart card. *Computers and Security*, 21(4):372–375, 2002.

[CLH04] Tzungher Chen, Wei-Bin Lee, and Gwoboa Horng. Secure SAS-like password authentication schemes. *Computer Standards & Interfaces*, 27(1):25–31, 2004.

[CW93] C. Chang and T. Wu. Remote password authentication with smart cards. *IEE Proceedings-E*, 138(3):165–168, 1993.

[FLZ02] L. Fan, J.H. Li, and H.W. Zhu. An enhancement of timestamp-based password authentication scheme. *Computers & Security*, 21(7):665–667, 2002.

[HL00] M. Hwang and L. Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, 2000.

[HLT02] M.S. Hwang, C.C. Lee, and Y.L. Tang. A simple remote user authentication scheme. *Mathematical and Computer Modelling*, 36(1):103–107, 2002.

[Lam81] Leslie Lamport. Password Authentication with Insecure Communication. *Communications of the ACM*, 24(11):770–772, 1981.

[LC05] N. Lee and Y. Chiu. Improved remote authentication scheme with smart card. *Computer Standards and Interfaces*, 27(2):177–180, 2005.

[LHY02] C. Lee, M. Hwang, and W. Yang. A flexible remote user authentication scheme using smart cards. *Operating Systems Review (ACM)*, 36(3):46–51, 2002.

[LKY04] S. W. Lee, H. S. Kim, and K. Y. Yoo. Improved efficient remote user authentication scheme using smart cards. *IEEE Transactions on Communications*, 50(2):565–567, 2004.

[SLH03a] J. Shen, C. Lin, and M. Hwang. A modified remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 49(2):414–416, 2003.

[SLH03b] J.J. Shen, C.W. Lin, and M.S. Hwang. Security enhancement for the timestamp-based password authentication scheme using smart cards. *Computers & Security*, 22(7):591–595, 2003.

[Sun00] H. Sun. An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(4):958–961, 2000.

[YRY05] E. J. Yoon, E. K. Ryu, and K. Y. Yoo. An improvement of Hwang-Lee-Tangs simple remote user authentication schemes. *Computers & Security*, 24(1):50–56, 2005.

[YS99] W.H. Yang and S.P. Shieh. Password authentication schemes with smart cards. *Computers & Security*, 18(8):727–733, 1999.