Cryptanalysis and Improvement of a Two-Factor User Authentication Scheme Providing Mutual Authentication and Key Agreement over Insecure Channels

Sajida Kalsoom and Sheikh Ziauddin

***Abstract*—A two-factor remote authentication scheme was presented by Chun-Ta Li *et al.* in 2010. We present the framework of an impersonation attack against their scheme if the smart card gets stolen. We show that it is easy for an attacker to compute password of a user by using information extracted from the stolen smart card. We also propose a simple and easy solution to fix this problem.**

***Index Terms*—Authentication schemes, cryptanalysis, mutual authentication, smart card.**

I. Introduction

To avoid unauthorized access, some security mechanism is needed to authenticate legitimate users. There are three common ways to authenticate a user: what you know (a pin or a password), what you have (a hardware token) and what you are (a biometric trait). The most commonly used mechanism for authentication is password. As it is not easy to remember strong passwords especially when a user has multiple accounts, this leads to either using same password for all accounts or selecting passwords with low entropy that can easily be guessed.

Hardware token-based schemes are also vulnerable because the hardware token can be lost, stolen, forged or compromised. Biometric-based authentication schemes are resistive for most of the problems in token-based and password systems and provide better security then the other two techniques, yet these are not widely adopted mainly because they are expensive to implement and use.

Due to the above-mentioned problems with the individual authentication techniques, researchers have proposed to use two-factor authentication where, in most cases, the two factors being used are a password and a hardware token typically a smart card. Using two-factors increases both security and reliability of the overall system. In this paper, we have analyzed one of the two factor authentication schemes proposed by Chun-Ta Li *et al.* [1] and discovered that it is vulnerable in case of loss of smart card. In a secure two-factor authentication scheme, it is not feasible for an attacker to defeat the schemes' security unless both factors are compromised. If an attacker can impersonate a user by stealing just one of the two factors, the scheme is considered insecure and broken. In Chun-Ta Li *et al.'s* scheme, as we will show shortly, compromise of one factor (smart card) leads to a straight forward compromise of the other factor (password). Having access to both the factors, it is trivial for the attacker to impersonate the user.

The remaining paper is organized as under. Section II presents related work. Section III describes Chun-Ta Li's protocol. Cryptanalysis is detailed in section IV. Section V discusses the proposed solution while conclusions of this work are presented in Section VI.

Manuscript received May 23, 2012; revised August 2, 2013.

The authors are with the Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan (e-mail: sajida.kalsoom@gmail.com, sheikh.ziauddin@comsats.edu.pk).

II. Related Work

The user has to send a valid login request to get access to the remote server. Most important concern is that this request must not disclose any secret information to the potential attacker. Therefore, a security mechanism is needed to successfully authenticate legitimate users without revealing any secret information. In 1981, Lamport [2] presented an authentication scheme which used verification tables stored at the server to authenticate its users. The major security hole in their scheme is that if the server gets compromised, the passwords of all the users are revealed. To address this issue, many schemes have been presented which do not maintain any verification table on server side. A remote authentication protocol was presented by Wu [3] not requiring any table on server side to verify passwords. Euclidean geometry is used as a basis for his scheme. He uses hash functions to secure the user's password. However, Hwang [4] later showed that Wu's scheme is susceptible to replay attack.

ElGamal public key cryptography was used by Hwang *et al.* [5] in their scheme. They use timestamp mechanism to guard against replay attacks. Hwang *et al.* [6] presented two-factor authentication scheme in which the users' passwords are not shown to server. In their scheme, passwords are selected freely. In addition, change of password is also allowed in their scheme. One way hash functions were used by Chien [7] in their remote mutual authentication scheme. Unfortunately, their scheme is susceptible to insider attack as shown by Chen [8]. Chen also provides his own scheme claiming to remove the security flaws in Chien's scheme. However, Hsu analyzed Chen's scheme and showed that it is susceptible to parallel session attack. Later, Yoon [9] claimed to improve Chen's scheme but, unfortunately, Hsiang and Shih [10] showed that Yoon's scheme is also vulnerable to certain attacks including impersonation, off-line password-guessing and parallel session. They also provide their scheme by resolving security flaws in the original Yoon's scheme.

DOI: 10.7763/IJMLC.2013.V3.348

A dynamic ID-based remote authentication protocol was presented by Das *et al.* [11]. In their scheme, no table is maintained to verify users. However, Wang *et al.* [12] later showed that Das' scheme does not provide two-way authentication resulting in server impersonation attack. They also show that, in case of smart card theft, the attacker can choose any random password to impersonate the user. Hwang *et al.* [6] presented a remote authentication protocol using password and smart card but Yoon *et al.* [13] showed that their scheme is susceptible to denial of service attack and it provides only uni-directional authentication. Yoon *et al.* also provide an improved version of Hwang's protocol. Recently, Chun-Ta Li *et al.* [1] found that Yoon's scheme is still susceptible to DoS attack due to unilateral authentication. Li *et al.* presented an improved scheme which provides mutual authentication. A common session key is used for communication and a nonce mechanism is used to prevent replay attacks. Unfortunately, we found that user impersonation attack can still be launched against their scheme if smart card is lost. Data stored on the smart card reveals confidential information and using that information, password can be computed. Next section gives a brief review on Chun Ta Li *et al.* scheme.

III. Chun-Ta Li et al. Scheme

Table I shows all notations we used in our paper.

TABLE I: Notations Used in This Paper

Notations	Description
U_c	User
S_i	Remote server
ID_c	Identity of the user
Pw_c	Password
$\oplus$	XOR
x	Server's Secret
T_{TSA}	Timestamp given by trusted time stamping authority TSA
N_c	User's generated nonce
N_s	Server's generated nonce
Sk	Common session key

Chun-Ta Li *et al.* [1] use password and smart card to authenticate users. They claim that their scheme provides key agreement in addition to providing two-way authentication. They use nonce mechanism to protect against replay attacks so that there is no need to use synchronized clocks. Chun-Ta Li's scheme consists of three phases which are explained below.

A. Registration Phase

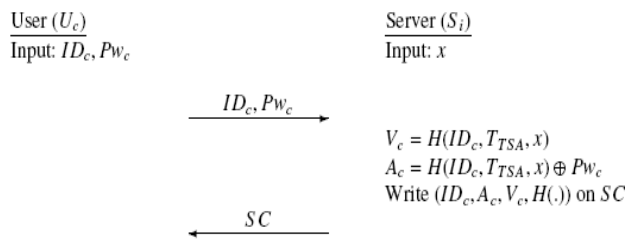

Fig. 1. Messages passed in Chun-Ta Li scheme at registration time.

In order to register with the remote server S_i, the user U_c submits ID_c and Pw_c to S_i. Afterwards, S_i performs the following tasks.

1) Calculates $V_c=H(ID_c, T_{TSA}, x)$.
2) Calculates $A_c = H(ID_c, T_{TSA}, x) \oplus Pw_c$.
3) Stores $(ID_c, V_c, A_c, H(.))$ on smart card.

The Registration phase is graphically represented in Fig. 1.

B. Login Phase

In order to login to remote server S_i, U_c enters her/his smart card and provides ID_c and Pw_c. Then smart card carries out the following tasks.

1) Calculates $B_c= A_c \oplus Pw_c$.
2) Checks whether $B_c = V_c$. If the test fails, request is rejected.
3) Calculates $C_1= B_c \oplus N_c$.
4) Sends (ID_c, C_1) to the server.

Fig. 2 provides a graphical representation of the login phase.

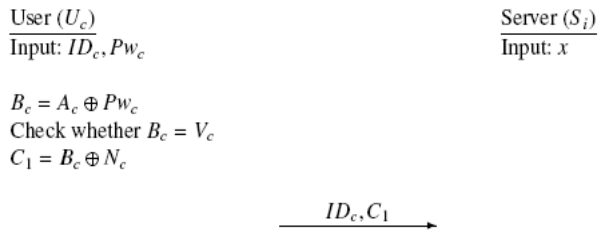

Fig. 2. Messages passed in Chun-Ta Li scheme at registration time.

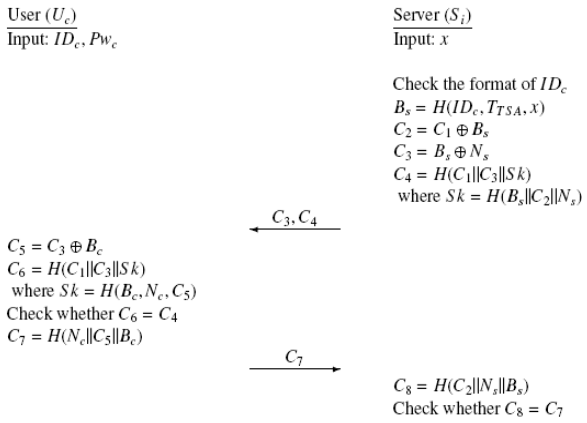

Fig. 3. Messages passed in Chun-Ta Li scheme at registration time.

C. Authentication Phase

When S_i receives a login request (ID_c, C_1), it performs the tasks as detailed below.

1) Tests ID_c format. Login request is rejected, if the format is incorrect.
2) Calculates B_s=H (ID_c, T_{TSA}, x).
3) Calculates $C_2= C_1 \oplus B_s$.
4) Calculates $C_3= B_s \oplus N_s$.
5) Calculates C_4=H(C_1 || C_3||Sk)

where Sk=H(B_s || C_2|| N_s) is the common session key.

6) Sends $\{C_3, C_4\}$ to U_c to achieve unilateral authentication.

Upon receiving $\{C_3, C_4\}$ from server, user carries out the tasks as detailed below.

1) Computes $C_5= C_3 \oplus B_c$ and C_6=H(C_1 || C_3|| Sk)

where Sk= H(B_c || N_c || C_5) is the common session key.

2) Checks whether (C_6= C_4). If the check is passed, U_c authenticates the sever and unilateral authentication is completed; otherwise U_c rejects the request.
3) Calculates C_7=H(N_c || C_5|| B_c) and sends C_7 to the server. Upon receiving C_7 from the user, the server carries out the following tasks.
1) Calculates C_8= H(C_2|| N_s|| B_s)
2) Checks whether C_8= C_7. If the values are equal, the server authenticates the user and mutual authentication is achieved.

Fig. 3 shows steps performed during authentication phase.

IV. Cryptanalysis of Chun-Ta Li et al.'s Scheme

Here, we detail a simple and straight-forward attack against Chun-Ta Li's scheme. We prove that their scheme is susceptible to a fatal security threat if smart card is stolen. In particular, we show that it is easy to find the password of any user if her smart card is accessed by an attacker. Once the password is known to the attacker, it is impossible for the system to differentiate between a legitimate user and a malicious person impersonating as a valid user.

The above-mentioned impersonation attack is feasible because due to sensitive information written on smart card, legitimate user's secrets become accessible. Once the smart card is compromised, the attacker can access the password, modify the password and impersonate the legitimate user.

Next, we will present our attack against Chun-Ta Li *et al.'s* scheme. The subsequent section shows that a part of sensitive information written on smart card is unnecessary and the scheme can be made secure by just removing that information from the smart card.

Our attack is based on a property of exclusive-or (XOR) operator namely if the application of XOR on two operands *A* and *B* results in *C* then XOR applied on *C* and *A* (resp. *B*) will result in *B* (resp. *C*). Mathematically, we can write

$$A \oplus B = C \implies A \oplus C = B \implies B \oplus C = A$$

In Chun-Ta Li *et al.'s* scheme, the user submits ID_c and Pw_c to S_i at registration time.

As it can be seen from Fig. 1, one of the calculations performed by the server S_i is given by

$$A_c = \mathrm{H}(ID_c, T_{TSA}, x) \oplus Pw_c$$

Now, because V_c=H(ID_c, T_{TSA}, x), therefore A_c= V_c $\oplus$ Pw_c and from the property of XOR, Pw_c = V_c $\oplus$ A_c. Again, as we see from Fig. 1, both the values A_c and V_c are written on smart card. Therefore, if an attacker steals user's smart card, it is a matter of a single XOR operation to get the user's password. Having access to both secrets of a particular user, it is easy for an adversary to communicate with the server masquerading as a legitimate user without having the possibly of being detected by the server. This will entirely defeat the security of the scheme and all the assumptions made for system's security will become void.

V. Proposed Solution

In this section, we propose a couple of small changes to overcome security vulnerabilities in Chun-Ta Li *et al.'s* scheme. The phase-wise changes are as follows.

A. Registration Phase

During registration phase of proposed scheme, smart card does not contain the value of V_c. The user U_c submits ID_c and Pw_c to S_i . Afterwards, S_i performs the following tasks.

1) Calculates A_c = H (ID_c, T_{TSA}, x) $\oplus$ Pw_c.
2) Stores (ID_c, A_c, H(.)) on smart card.

B. Login Phase

The only improvement in login phase is to leave out the check B_c = V_c, that is performed after calculating B_c on the user's end (see Fig. 2). Elimination of this check does not create any security issue and the rest of the scheme works appropriately. The operations performed by the user U_c at login time are now reduced to the following.

1) Calculates B_c= A_c $\oplus$ Pw_c.
2) Calculates C_1= B_c $\oplus$ N_c.
3) Sends (ID_c, C_1) to the server.

C. Authentication Phase

Authentication phase of the proposed solution remains exactly the same as that of the original Chun-Ta Li's scheme.

VI. Conclusion

This paper presents cryptanalysis of Chun-Ta Li's scheme. We pointed out security pitfalls in their scheme and showed that their scheme is susceptible to user impersonation attack when the smart card is compromised. The attack exists because the data written on smart card is enough to compute the password. To overcome this deficiency, we have proposed a solution which removes this security flaw and also inherits the merits of Chun-Ta Li's scheme.

References

[1] C. Li, C. Lee, and L. Wang "A two-factor user authentication scheme providing mutual authentication and key agreement over insecure channels," *Journal of Information Assurance and Security*, vol. 5, pp. 201-208, 2010.
[2] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770-772, 1981.
[3] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications*, vol. 18, pp. 959–963, 1995.
[4] M. Hwang, "Cryptanalysis of a remote login authentication scheme," *Computer Communications*, Elsevier, vol. 22, pp. 742-744, 1999.
[5] M. Hwang and L. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electronics*, New York: Institute of Electrical and Electronics Engineers, vol. 46, pp. 28-30, 2000.
[6] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, Elsevier, vol. 36, pp. 103-107, 2002.
[7] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Computers & Security*, vol. 21, pp. 372–375, 2002.
[8] K. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electronics*, vol. 50, pp. 204-207, 2004.
[9] E. Yoon, E. Ryu, and K. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electronics*, vol. 50, pp. 612, 2004.
[10] H. Hsiang and W. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," *Computer Communications*, Elsevier, vol. 32, pp. 649-652, 2009.

[11] M. Das, A. Saxena, and V. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Trans. on Consumer Electronics*, vol. 50, pp. 630, 2004.
[12] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, Elsevier, vol. 32, pp. 583-585, 2009.
[13] E. Yoon, E. Ryu, and K.Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication scheme," *Computers & Security*, Elsevier, vol. 24, pp. 50-56, 2005.

Sajida Kalsoom received her MCS degree from Arid Agriculture University Rawalpindi, Pakistan. She received her MS (CS) degree from COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan. Sajida is now a lecturer in the Dept. of Computer Science, CIIT, Islamabad, Pakistan. Her research interests include information security and image processing.

Sheikh Ziauddin received his BS degree in Civil Engineering from Bahauddin Zakariya University, Multan, Pakistan. He received his MS (CS) degree from Bahria University, Islamabad, Pakistan. He did his Ph.D. in Computer Science from Asian Institute of Technology in Bangkok, Thailand. He also completed a postdoctoral work from University of Nice, France. Ziauddin is an Assistant Professor in the Dept. of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan. His research interests include cryptography, computer security biometrics and image processing.