ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure Modification to Hsiang-SHIH'S Schema: A Case Study

Mohd Yousuf
Dept. of Computer science Engineering, Asifia College of Engineering and Technology, Hyderabad, India
yousuf.asifia@gmail.com

Abstract

The proposed schemes of Hsiang and Shih for the remote User authentication scheme using smart card they expropriate their schemes guarded against parallel session attack, and password guessing attacks, I, in this paper suggested that Hsiang and Shih's schemes are still in jeopardy to off-line password guessing attacks and imperceptible to on-line password guessing attacks. The scenario will be same in which the user loss smart card as in the schemes of Hsian and shih's. This proposal is a productive reconstruction and beat the security flaws in the Hsiang and Shih's remote user authentication schemes using smart cards.

Keywords:-Smart Card, Cryptanalysis, authentication, Security.

Introductions

As the spontaneous spread of communication network technology, it is extremely important to watch keen view to developing security concerns As such, password-based authentication has become one of the best practically applied techniques used to problem-solve regarding various applications in wireless environments and other remote authentication systems. In 1981, Lamport [13] proposed the first password-based remote authentication scheme for identifying a legal user using a hash-chain technique through insecure communication. In our scheme, all secret passwords are stored in a verifier's table that is maintained by the remote server; in a situation such as this, there exists a potential threat such that all maintained records might be modified by attackers. In order to solve these problems, numerous undertakings in research [1-10, 12, 14-19] have been executed during recent years. In 1990, Hwang et al. [10] proposed a non-interactive password authentication scheme without password tables using smart cards. Follow up research [1, 2, 8, 11, 13, 16, 17] has also been proposed. Because these schemes suffered from a susceptibility to ID-theft attack, an attacker could forge a legal user using an eavesdropped users' identity documentation. Yoonetal.[20], in 2004, proposed an efficient password based remote user authentication scheme using smart cards that has significant advantages; most notably, the remote server does not need to maintain a verifier's table. However, in 2009, Hsiang and Shih [6] pointed out that Yoon et al.'s scheme still exhibited several weaknesses. For example, it is susceptible to parallel session attacks, masquerade attacks and password guessing attacks. Nevertheless, according to my cryptanalysis, Hsiang and Shih's scheme still has notable weaknesses to off-line password guessing attacks and undetectable on-line guessing attack. Moreover, the smart-card-based schemes suffered in contexts involving a lost smart card. In fact, some researches [11, 15] reveal the stored parameters of smart card. Therefore, I propose an improved scheme to overcome all of the security weaknesses mentioned above. The rest of this paper is organized as follows. Section 2 provides a brief review of the weakness of Yeh et al.'s schemes. Section 3 provides details of the proposed scheme. Section 4 provides a security analysis of my scheme. Section 5 shows a security and performance comparison with related research. I provide conclusions in the last section.

Review of hsiang and shih's scheme

In this section, we briefly describe Hsiang and Shih's scheme [6], which consists of four phases: the registration phase, the login phase, the authentication phase, and the password change phase. The notation of this paper is listed as follows:

U	: the user
S	: the remote server
Tu,Ts	: the timestamps
ID	: the user's identity
PWD	: the user's password
x	: the secret key of remote server
b	: random numbers
Nu, Ns	: nonces
$h(\cdot)$	: a one-way hash function
$\oplus$	: bitwise exclusion operation
$\|\|$	: concatenation operation

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

?
$X = Y$: determine X if equal to Y

A. Registration phase

In this phase, U initially registers, or re-registers, to S and the steps are described as follows:

Step 1:
U selects a random number b and computes $h(b \oplus PWD)$. He or she then securely send ID, $h(PWD)$ and $h(b \oplus PWD)$ to S.

Step 2:
S creates a new entry with a value m=0 for U in the database or sets m=m+1 in the existing entry. Here, m denotes the number of times of re-registering to S for each user U. Next, S computes EID, P, R and V:
$EID = (ID \,||\, m)$ (1)
$P = h(EID\ x)$ (2)
$R = Ph(b\ PWD)$ (3)
$V = h(Ph(PWD))$ (4)
to U.

Step 3:
Finally, U enters a random number b into his or her smart card.

B. Login phase

When U wants to login S, the following steps will be performed:

Step 1:
U inserts his or her smart card into the card reader and then enters the ID and PWD.

Step 2:
U's smart card computes $C1$, $C2$:
$C1 = R \oplus h(b \oplus PWD)$ (5)
$C2 = h(C1 \oplus Tu)$ (6)
and sends the authentication request messages (ID, Tu, $C2$) to S.

C. Authentication phase

Upon receiving the request messages (ID, Tu, $C2$), the remote server S and the smart card perform the following steps:

Step 1:
S first checks the validity of $h(ID)$ and $Ts > Tu$. If it does not hold, S rejects U's login request; otherwise, S computes $h(h(EID \oplus x) \oplus Tu)$, and compares it with $C2$:

$h(h(EID \oplus x) \oplus Tu) =? C2$ (7)
If the Eq. (7) holds, S accepts U's login request and computes $C3$: C3 =h(h(EID$\oplus x$) $\oplus$ h(Ts)) (8) otherwise, S rejects it. Continuously, S sends the response messages (Ts, $C3$) to U.

Step 2:
According the received messages (Ts, $C3$), U's smart card checks the validity of $Ts > Tu$. If it does not hold, U terminates the session; otherwise, U computes $h(C1 \oplus h(Ts))$ and compares it with $C3$: $h(C1 \oplus h(Ts)) =? C3$ (9)
If the Eq. (9) holds, U successfully authenticates S.

D.Password change phase

In this phase, U intends to exchange his or her password PWD with a new one $PWDnew$. The steps are described as follows:

Step 1:
U inserts his or her smart card into the card reader, enters ID and PWD, and then requests a password change.

Step 2:
U's smart card computes P^*, V^* and compares V^* with the stored V:
$P^* = R \oplus h(b \ h(\oplus(PWD)))$ (10)
$V^* = h(P^* \ h(\oplus(P \oplus WD)))$ (11)
$V^* =? V$ (12)
If Eq. (12) does not hold, the smart card rejects the request; otherwise, U inputs the new password $PWDnew$. Afterward, U's smart card computes $Rnew$ and $Vnew$ as follows:
$Rnew = P^* \oplus h(b \ h(\oplus(PWDnew)))$ (13)
$Vnew = h(P^* \oplus h(\ (P \oplus WD)))$ (14)
then, replaces R and V with $Rnew$ and $Vnew$, respectively.

Weakness of hsiang and shih's scheme

Although Hsiang and Shih's scheme was an improvedversion of Yoon et al.'s scheme [20], several security weaknesses still exist. These susceptibilities include: off-line password guessing attacks and undetectable on-line password guessing attacks. We describe these attacks as follows.

A. Off-line password guessing attacks

This involves a situation where a user's smart card was stolen by an attacker A, and where A uses the stolen smart card to extract the secret parameters b and R [11, 15]. Continuously, A can use the previously eavesdropped messages (ID,

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Tu, *C*2) or (*Ts*, *C*3) to obtain *U*'s password *PWD* according to the following steps:

Step 1:
First, an attacker *A* guesses a password *PWDA* and computes counterfeit messages *CA*1 or *CA*2 for comparison with the intercepted messages *C*2 or *C*3, as follows:
CA1=h(R⊕*(b*⊕*PWDA)* ⊕*Tu)* (15)
CA1=? C2 (16) or
CA2=h(R⊕*(b*⊕*PWDA)* ⊕*h(Ts))* *(17)*
CA2?=C3 *(18)*

If the Eq. (16) or (18) holds, the attacker *A* guessed the correct *PWD*; otherwise, A can retry step 1 until the Eq. (16) or (18) be held. Therefore, A can guess the correct PWD to change the user's password. Refer to the password change phase.

B. Undetectable on-line password guessing attacks

This refers to upon subsection, where an attacker *A* is able to extract the secret parameters *b* and *R* through the stolen smart card. As with the previously eavesdropped messages (*ID*, *Tu*, *C*2), *A* can guess the *U*'s password as follows:

Step 1:
A guesses a possible password *PWDA* and computes a value following Eq. (15) *CA*1 with a timestamp *TA*. *A* then computes counterfeit messages (*ID*, *TA*, *CA*1) to send to the server *S*.

Step 2:
After receiving the messages, *S* first checks the timestamp *Ts* > *TA*. Continuously, *S* computes *h*(*h*(*EID* ⊕*x*) ⊕*TA*) to compare the received value *CA*1. If both of them are equal, then *PWDA* is *U*'s correct password. Then, *S* accepts this login request and sends the messages (*Ts*, *C*3) to *A*.

Step 3:
According to the received messages, *A* can recognize that the correct password has been guessed; otherwise, *A* retries the above attack procedures until obtaining the correct password.

Ourimproved scheme

In the context of Hsiang and Shih's remote user authentication scheme, the server's secret key is compromised by a malicious legal user. Therefore, we have designed a scheme with two unknown factors to protect each parameter in the smart card. Our remediable schemes consist of four phases: the registration phase, the login phase, the authentication phase, and the password change phase. We describe these phases in the following subsection.

A. Registration phase
Step 1:
The user *U* chooses a password and then submits the registration messages (*ID*, *h*(*PWD*)) to the remote server S via a secure channel.

Step 2:
When *S* receives the registration messages from *U*, *S* first generates a nonce *Ns* and uses *ID* and *h*(*PWD*) to compute three values *P*, *R* and *V*:
P=h(x) ⊕*((ID)||Ns)* (24)
R= h(x||Ns) h((⊕*PWD))* (25)
V=h(ID||h(x)||Ns)) (26)
Afterward, *S* issues the smart card with parameters *P*, *R*, *V* and *h*(·) to *U* through a secure channel.

B. Login phase
Her password, he or she will perform the following steps:
Step 1:
U inserts his or her smart card into a card reader or the terminal, and then enters the *ID* and the original *PWD*.
Step 2:
According to Eqs. (28) and (29), the smart card examines the validity of *ID* and *PWD* and compares *V'* with the stored *V*. If this holds, *U* is allowed to key in a new password *PWDnew*; otherwise, the smart card rejects the password change request.
Step 3: The smart card calculates *R'*:
R'=R⊕*h((PWD))* ⊕*h(*⊕ *(PWD new))*
= h(x||Ns) *h(*⊕*(PWD new))* (37)
and replaces the old value *R* with the new *R'*. Thus, the password has been successfully changed without the participation of remote server *S*.

Security Analysis

In this section, we will discuss the security of our improved scheme and demonstrate how it is more secure than previous schemes.

A. Mutual authentication

In our improved scheme, the server authenticates the user by checking the message *C*2. If server's computed value (*h*(*ID'*)||*Nu'*) is equal to *C*2, the server proves that the user is valid. Then, server sends message *C*3 to the user. The user also compares *C*3 with his or her computation value *h*(*ID*||*Nu*). If both of them are equal, the user confirms that the server is legitimate. Since the secret

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

value $h(x||Ns)$ is shared between user and server, they can authenticate each other with the login messages (P, $C1$, $C2$) and the reply message $C3$. Hence, mutual authentication obtains in our improved scheme.

B. Smart card lost

According to our improved scheme, if an attacker A obtains a legal user U's smart card somehow, they cannot obtain any parameter without the user's password; even if A extracts the parameters P, R, and V (see Eqs. (24)-(26)) from the smart card, they still cannot obtain any sensitive information (such as ID, PWD, Ns or the server's secret key x) with those parameters. Notably, A does not know U's correct password and each parameter are always protected by two unknown factors of the smart card. Therefore, no one can use the stolen smart card to obtain authentication without U's correct password and identity.

C. Password guessing attacks

This situation involves an attacker A obtaining the U's smart card and intercepting previous messages. In this case, A intends to guess the U's PWD from the stored parameter R of the smart card and must know the secret key x and the nonce Ns to compute similar parameters for comparison with parameter R. On the other hand, A can use R and the intercepted P to compute similar messages (P, $C1'$, $C2'$) and send it to S in an attempt to guess U's PWD. As A has two unknown values, ID and PWD, it is difficult to successfully complete this password guessing attack.

D. Replay attack

In our improved scheme, we use a nonce mechanism to prevent the replay attack and to solve the synchronization problem. When an attacker intends to replay the previous messages (P, $C1$, $C2$) to achieve authentication, they cannot as the nonce value Nu is different in each session. For this reason, the attacker cannot achieve authentication using previous messages.

Performance analysis

Recently researchers [6, 20] have generally only considered one unknown factor for each parameter; this is why their schemes were compromised and have become susceptible to various attacks. However, our improved scheme always consists of two unknown factors within each communication to meet more stringent security requirements. It can be clearly observed that our scheme is more secure than those proposed by others. Generally speaking, the computation cost of our scheme is comparable to Hsiang and Shih's scheme. However, our scheme can defend against all of the attacks discussed herein more effectively than all previous attempts. We compare the security requirements and computation costs with Hsiang and Shih's scheme in Table respectively

Table . **Performance Comparision Between Other Related Researches And Ours**

	Yoon et al.'s scheme [20]	Hsiang and Shih's scheme[6]	sours
Registration Phase	$2H + 3Xor$	$4H + 4Xor$	$4H + 2Xor$
Login and authentication phase	$6H + 7Xor$	$8H + 7Xor$	$10H + 4Xor$
Password change phase	$6H + 6Xor$	$6H + 6Xor$	$3H + 2Xor$
Total	$14H + 16Xor$	$18H + 17Xor$	$17H + 8Xor$

Conclusions

In this paper, we have proposed an improved scheme that consistently protects each secret parameter with two unknown factors in the smart card; thus, an attacker cannot obtain any sensitive information, even if he or she is a malicious legal user. Most notably, our scheme not only addresses more stringent security requirements and protects against known types of attacks, it also reduces computation costs more effectively than Hsiang and Shih's scheme. Therefore, our scheme holds substantial value in the context of numerous applications in various network environments.

Acknowledgment

This work is to enable better security for remote user authentication in a secure network access by multiple user connected.

References

1. *K. Awasthi, and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp. 1246-1248, 2003.*
2. *C.Chang, and K. F.Hwang, "Some forgery*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

attacks on a remote user authentication scheme using smart cards," Informatics, Vol. 14, No. 3, pp. 289-294, 2003.

3. *H. Y. Chien, and C. H. Chen, remote authentication scheme preserving user anonymity," In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, pp. 245-248, 2005.*
4. *Y. Ding, and Horster, P., "Undetectable on-line password guessing attacks," ACM SIGOPS Operating Systems Review, Vol. 29, No. 4, pp. 77-86, 1995.*
5. *X. Duan, J.W.Liu, and Q. Zhang, "Security improvement on Chienet al.'s remote user authentication scheme using smart cards," In:Proceedings of the IEEE International Conference on Computational Intelligence and Security, pp. 1133-1135, 2006.*
6. *H.C.Hsiang, and W.K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications, Vol. 32, No. 4, pp. 649-652, 2009.*
7. *M. S.Hwang, S. K.Chong, and T. Y.Chen, "DoS-resistant ID-based password authentication scheme using smart cards," Journal of Systems and Software, Vol. 83, No. 1, pp. 163-172, 2010.*
8. *M. S.Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," Mathematical and Computer Modelling, Vol. 36 No. 1-2, 103-107, 2002.*
9. *M. S. Hwang and L. H. Li, "A new remote userauthentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, 2000.*