스마트카드를 이용한 원격 사용자 인증 구조

Remote User Authentication Scheme using Smart Cards

최종석, 신승수
동명대학교 정보보호학과

Jong-Seok Choi(bestofcom@gmail.com), Seung-Soo Shin(shinss@tu.ac.kr)

요약

2005년에 Chien과 Chen 은 Das et al. 구조의 문제점을 해결하고 사용자 익명성을 보장하기 위한 원격 사용자 인증구조를 제안하였다. 2007년에 Hu et al.은 Chein과 Chen의 구조는 몇 가지 문제점을 가진다고 지적하였다. 그리고 그들은 새로운 구조를 제안하고 그들의 구조는 자신들이 Chien과 Chen 구조에 대해 지적한 모든 문제점을 극복하였다고 주장했다. 그러나 우리는 Hu et al. 구조도 여전히 서비스 거부 공격과 사용자 익명성을 보장하지 못한다는 문제점을 가지고 있다는 것을 보여 줄 것이다. 그리고 우리는 우리의 구조를 제안하고 제안한 구조에 대한 안전성을 분석했다.

■ 중심어 : | 인증 | 익명성 | 스마트카드 |

Abstract

In 2005, Chien and Chen proposed a remote user authentication scheme for preserving user anonymity to conquer some problems Das et. al. schemes have. In 2007, Hu et. al. pointed out that their scheme have some problems. Therefore, they proposed a new one and claimed that their scheme overcome all of these problems. However, We will show that Hu et. al. scheme still hold some problems; it cannot resist to denial of service attack and protect the user anonymity. Hence, we propose ours and demonstrate our scheme conquer these problems.

■ keyword : | Authentication | Anonymity | Smart Cards |

I. Introduction

Entity authentication is an important way to ensure the security of the communication when a user logins a remote server by network. In 2005, Chien and Chen [1] pointed out that Das et. al.[2] scheme fails to protect the user's anonymity. However, in 2007, Hu et al[3]. found that Chien and Chen's scheme is vulnerable to some attacks[4-6] and proposed a new one. However, we will demonstrate that Hu et. al.'s scheme also has some problems. Therefore, we will propose an improved scheme to conquer these problems and describe ours. This paper is organized as Section 3 points out its problems. And follows. Section 2 briefly reviews Hu et. al.'s scheme, then Section 4 presents our scheme, Section 5 analyzes the our security. Finally, Section 6 gives a conclusion.

접수번호 : #081204-002
접수일자 : 2008년 12월 04일
심사완료일 : 2009년 01월 07일
교신저자 : 신승수, e-mail : shinss@tu.ac.kr

II. Review of Hu et al. scheme

In this section, we will show Hu et. al. scheme cannot fail to protect problems. It depends on counters instead of synchronized clocks to time stamp messages so that the recipients can verify the timeliness of the messages and recognize and reject replays of messages communicated in the past. The scheme sets counters N_u and N_s in user's and server's side respectively. N_u and N_s are synchronized normally, and their initial values are 0. Moreover, since the operation of password change is not explicitly specified in Chien and Chen's scheme, the scheme additionally involves it for completeness. Hu et. al. scheme performs as follows.

We will use throughout notations as [Table 1] in this paper.

Table 1. Parameters

Symbol	Description
U	the user
ID	the identity of U
PW	the password of U
S	the remote system
x	the strong secret key of S
h()	a secure one-way hash function
p, g	the parameters of Diffie-Hellman key exchange protocol
⊕	the exclusive-or (XOR) operation
=>	secure channel transfer
→	common channel transfer

1. Registration phase

This phase is invoked whenever U initially registers or re-registers to S.

Step R1. U chooses a password PW, generates a random number t, then computes $h(t \oplus PW)$.

Step R2. U=>S: ID, h(t ⊕ PW).

Step R3. If it is U's initial registration, S creates an entry for U in the account database and stores ID, Ns in this entry. Otherwise, S updates the existing entry for U. Next, S computes I = h(ID⊕x), M = I ⊕ h(x) and m = M ⊕ h(t⊕PW) = h(ID⊕x) ⊕ h(x) ⊕ h(t⊕PW).

Step R4. S=>U : a smart card containing ID, m, I, M and the public parameters (h( ), p).

Step R5. U enters t into his/her smart card. Note that U's smart card contains ID, m, I, M, t, p and h(), and U does not need to remember t after finishing Step R5.

2. Login phase

This phase is invoked whenever U wants to login S.

Step L1. U inserts his/her smart card to the card reader of a terminal, and inputs his/her ID and PW.

Step L2. After checking the validity of the ID and verifying M ⊕ h(t⊕PW) equals the stored m, the smart card generates a random number $r_u = g^a$ mod p, then computes R = h(I⊕ r_u) and C = I ⊕ M ⊕ R = h(x) ⊕ R.

Step L3. U → S : {C, E_R[r_u ID, Nu]}, where the E_R[r_u, ID, Nu] is a ciphertext of [r_u, ID, Nu] encrypted using the secret key R.

3. Authentication phase

This phase is invoked whenever S receives U's login request.

Step A1. S computes R = C ⊕ h(x), then decrypts the message E_R[r_u, ID, Nu].

Step A2. After checking the validity of the ID, S compares the decrypted data Nu with the corresponding Ns. If they are equal, S continues the next step. Otherwise, S gives a synchronization signal to U, and U must send an authentication request message to synchronize Nu with Ns.

Step A3. S computes I = h(ID ⊕ x) and verifies whether the following equation holds, R = h(I ⊕ r_u). If it holds, S accepts the service request and sets Ns = Ns + 1. Otherwise, rejects it.

Step A4. S → U : E_R[I⊕ r_s, r_u⊕ Ns], where $r_s = g^b$ mod p.

Step A5. Upon receiving the message E_R [I ⊕ r_s , r_u ⊕ Ns], U checks whether decrypted data contains the value r_u ⊕ (Nu +1). If so, U computes r_s = I ⊕ (I ⊕ r_s) and sets Nu = Nu + 1, and then U can generate the session key Kus = $r_s^a = g^{ab}$ and deliver secret information with server.

4. Password change phase

This phase is invoked whenever U wants to change his/her password PW with a new one, say PW*.

Step P1. U inserts his/her smart card into the smart card reader of a terminal. He/she submits the password PW and requests to change the password.

Step P2. The smart card verifies whether M ⊕ h(t ⊕PW) equals the stored m. If they are equal, then U can enter PW*; otherwise, it rejects the password change request.

Step P3. U's smart card computes m* = m ⊕ h(t⊕ PW) ⊕ h(t⊕PW*), which yields M ⊕ h(t⊕PW*), and then replaces m with m*.

Since the password change operation is performed only within U's smart card, U doesn't need to inform S.

III. Problems of Hu et. al. scheme

They claimed that their scheme explicitly conquer all of mentioned problems in their paper. But, we have found that theirs also have problems as follows.

1. The user anonymity

We have seen their scheme to inform ID to the server, and ID disclosed from anyone, since anyone can know the secret key R and decrypt the message [r_u , ID, Nu], and then finally look at ID. So, we wonder if the scheme can keeps the user anonymity, because anyone can compute R = C ⊕ h(x) and know the user's ID. Finally, we will adopt hash-function over ID with a random number t for the problem. Therefore, the server cannot even know who one requests a service to the server and guarantee the user anonymity.

2. Denial of service attack

They pointed out that the schemes using time stamp protecting restricted replay attack are generally regard as vulnerable from denial of service attack, because of the server has to check whether a message is the validity, if yes, the server continue next step, otherwise, reject the message. Therefore, they have used only the encrypted counter for checking the validity of the message and have claimed that their scheme archive to defend the attack. However, although the scheme have used only the encrypted counter, it is none the more as Chien and Chen not defending the attack. In Hu et al. scheme, the attacker can decrypt the message of the user E_R [r_u , ID, Nu] and change the value of Nu. Hence, the message cannot pass Step A2. If the attacker infinitely repeat the behavior like that, the server will also continuously reject this message. Therefore, the user will not be provided for the service from the server by this attack forever.

IV. Our scheme

In this section, we will propose our scheme that is composed of registration phase, login phase, authentication phase and password changing phase and perform as follows.

1. Registration phase

This phase is invoked whenever U initially registers or re-registers to S

Step R1. U chooses a password PW and ID, generates a random number t, then computes h(PW⊕t) and h(ID⊕t).

Step R2. U=>S: h(ID⊕t), h(PW⊕t).

Step R3. S creates and updates an entry for U in the account database, in accordance whether it is U's initial registration. Next, S computes I = h(ID⊕t), M = I ⊕ h(x) and m = h(ID⊕t) ⊕ h(x) ⊕ h(PW⊕t), and then store I, Ns in database. At this time, S obtain a random index IND of a database of the user, and then compute i = IND ⊕ x.

Step R4. S=>U: a smart card containing m, i, I, M and the public parameters (h( ), p).

Step R5. U enters t into his/her smart card. Note that U's smart card contains m, i, I, M, t, p and h( ), and U does not need to remember t after finishing Step R5.

2. Login phase

This phase is invoked whenever U wants to login S.

Step L1. U inserts his/her smart card to the card reader of a terminal, and inputs his/her ID and PW.

Step L2. After checking the validity of the h(ID⊕t) and verifying whether M ⊕ h(PW⊕t) equals the stored m, the smart card generates a random number $r_u = g^a$ mod p, then computes R = M ⊕ I ⊕ r_u = h(x) ⊕ r_u and C = M ⊕ r_u = h(ID ⊕ t) ⊕ h(x) ⊕ r_u.

Step L3. U → S : {i, C, E_R [r_u , I, Nu]}, where the E_R [r_u , I, Nu] is a ciphertext of [r_u , I, Nu] encrypted using the secret key R.

3. Authentication phase

This phase is invoked whenever S receives U's login request.

Step A1. S computes IND = i ⊕ x and obtain I from the database that has the random index IND

Step A2. S computes R = C ⊕ h(ID ⊕ t) = C ⊕ I, then decrypts the message E_R [r_u , I, Nu].

Step A3. S compare R in Step A1 with C ⊕ I in the decrypted data E_R [r_u , I, Nu].

Step A4. S compares N_u with the corresponding N_s. If they are equal, S continues the next step. Otherwise, S gives a synchronization signal to U and U must send an authentication request message to synchronize N_u with N_s.

Step A5. S → U : E_R [$I \oplus r_s$, $r_u \oplus Ns$], where $r_s = g^b$ mod p, and $K_{us} = r_u^b = g^{ab}$ mod p.

Step A6. Upon receiving the message E_R [I ⊕ r_s , r_u ⊕ Ns], U checks whether decrypted data contains the value r_u ⊕ (Nu+1). If so, U computes r_s = (I ⊕ r_s) ⊕ I and sets Nu = Nu + 1, and then U can generate the session key Kus = $r_s^a = g^{ab}$ mod p and deliver secret information with server.

4. Password change phase

This phase is invoked whenever U wants to change his/her password PW with a new one, say PW*.

Step P1. U inserts his/her smart card into the smart card reader of a terminal. He/she submits the password PW and requests to change the password.

Step P2. The smart card verifies whether $M \oplus h(PW \oplus t)$ equals the stored m. If they are equal, then U can enter $PW*$, otherwise, it rejects the password change request.

Step P3. U's smart card computes $m^* = m \oplus h(PW \oplus t) \oplus h(PW^* \oplus t)$, which yields $M \oplus h(PW^* \oplus t)$, and then replaces m with m*.

Since the password change operation is performed only within U's smart card, U does not need to inform S.

V. Security analysis

1. Strong masquerading server/user attack

In 1999, Kocher et al. [7] stated that all existing smart cards were vulnerable in that the secret keys stored in the smart card could be extracted by monitoring the power consumption. In 2002, Messerges et al. [8] showed that the secrets stored in a smart card may be breached by analyzing the leaked information.

In fact, defending this attack is easy. In order to completely block this attack, we have adopted the way and the secret key R is computed by ID with a random number t and $h()$ that is not inform to anyone. $h(ID \oplus t)$ as the secret key with the server/user is used to create R from C, and is stored in the server's database and the user's smart card. Therefore, if the server's database has been conquered by the attacker, our scheme is secure from this attack.

2. Insider attack

Since U registers to S by presenting $h(PW \oplus t)$ instead of PW, the insider of S can not directly obtain PW. Furthermore, as t is not revealed to S, the insider of S can not obtain PW by performing an off-line guessing attack on $h(PW \oplus t)$ [9]. Thus, the improved scheme can resist the insider attack [10].

3. Denial of service attack

Similarly, We have used only the encrypted counter. If anyone wants to change counter, they have to decrypt the data and input disguised counter. However, the attacker cannot know the another user's $h(ID \oplus t)$. Therefore, We can state that the scheme is secure against this attack but that the legal own user input wrong counter by intent by him/herself.

4. Restricted replay attack

We employ two counters instead of time stamp to resist the restricted replay attack. So neither the replay of an old login message $\{i, C, E_R[r_u, ID, \mathrm{N}]$ of U nor the replay of S's response message $E_R[I \oplus r_s, r_u \oplus N_s]$ will work, as it will fail in Step A2 and Step A5 due to the counter checking respectively in our scheme.

5. Password detection

Since the smart card can verify PW using the stored m in Step L2, the wrong password will be quickly detected by the smart card once a wrong password input occurs. That is, our scheme provides timely password verification. Similarly, when the smart card was stolen, unauthorized users cannot change the password of the smart card [11] because the smart card can verify PW using the stored m in Step P2. So the password change phase of our scheme is secure.

6. The user anonymity

Our scheme use $h(ID \oplus t)$ instead of ID. Therefore, anyone cannot surely know the user's ID which the server cannot even know. In addition, since we have adopted ID with $h()$ and the random number t, anyone cannot guess the user's ID. And, we advise the server to use a random index of the database for the user. Finally, we have claimed that the scheme completely preserve the user anonymity.

VI. Comparisons

1. Performance

Our scheme needs two extra XOR and one extra hash-function only for registration phase. The registration phase does not influence any phase. Hence, our scheme dose not decreases performance than Hu et al. scheme except registration that is invoked only whenever the user want registration to the server.

[Table 1] says that our scheme is the same performance with Hu et al. scheme because of registration phase is invoked only once.

Table 1. Comparison of performance with Hu et al

	Hu et al Scheme	Our Scheme
Registration	3⊕, 2h	5⊕, 3h
Login	3⊕, 1pow, 1E	3⊕, 1pow, 1E
Authentication	2⊕, 2pow, 1E	2⊕, 2pow, 1E
Password Change	3⊕	3⊕

⊕ : XOR Bit-operation, h : Hash function, pow :Power operation, E : Encryption

2. Functionality

Our scheme overcome some problems, which Hu et al. scheme has, by the same computation price but registration phase. [Table 2] says that our scheme is secure on Strong masquerading server/user attack, Insider attack, Denial of service attack, Restricted replay attack, Fast password detection and The user anonymity.

Table 2. Comparison of Functionality with others

	(1)	(2)	(3)	(4)	(5)	(6)
Ours	yes	yes	yes	yes	yes	yes
Hu	yes	yes	no	yes	yes	no
Chien	no	no	no	no	no	no

(1) Strong masquerading server/user attack, (2) Insider attack, (3) Denial of service attack, (4) Restricted replay attack, (5) Fast password detection, (6) The user anonymity

VII. Conclusion

The threat of smart card security [12][13] is a crucial concern, where some secret information is stored in memory of smart cards.

In the paper, we have shown the problems of Hu et. al. scheme, and have proposed a new one that keeps the advantage of Hu et. al. scheme; It is fast wrong password detection, the operation of password changing. In addition, our scheme guarantees denial of service attack of the illegal user and the attacker who is not the own user of the message and the user anonymity by using $h(ID \oplus t)$. Therefore, our scheme conquer the mentioned problems of Hu et. al. scheme. Futhermore, we recommended the course of the kind of this scheme to exert to research to involve and provide various functions and convenience using the smart card then researches on the attacks.

참 고 문 헌

[1] H. Y. Chien and C. H. Chen, "A remote authentication scheme preserving user anonymity," IEEE AINA'05, Vol.2, pp.245-248, 2005(3).

[2] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Trans. On Consumer Electronics, Vol.50, No.2, pp.629-631, 2004.

[3] Hu, Yang and Niu, "Improved Remote User

Authentication Scheme Preserving User Anonymity," IEEE CNSR'07, 2007.

[4] W. C. Ku, C. M. Chen, and H. L. Lee, "Crypt-analysis of a variant of Peyravian-Zunic's password authentication scheme," IEICE Trans. Commun., Vol.E86-B, No.5, pp.1682-1684, 2003(5).

[5] H. M. Qiu, Y. X. Yang, and Z. M. Hu, "A new mutual user authentication scheme using smart card," Application Research of Computers, No.12, pp.103-105, 2005.

[6] E. J. Yoon and K. Y. Yoo, "More efficient and secure remote user authentication scheme using smart cards," IEEE ICPADS'05, Vol.2, pp.73-77, 2005(7).

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Proc. Advances in Cryptology (CRYPTO'99), pp.388-397, 1999.

[8] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Trans. on Computers, Vol.51, No.5, pp.541-552, 2002(5).

[9] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electronics, Vol.50, No.1, pp.204-207, 2004(2).

[10] W. C. Ku, C. M. Chen, and H. L. Lee, "Cryptan- alysis of a variant of Peyravian-Zunic's password authentication scheme," IEICE Trans. Commun., Vol.E86-B, No.5, pp.1682-1684, 2003(5).

[11] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electronics, Vol.50, No.2, pp.612-614, 2004(5).

[12] M. Joye and F. Oliver, "Side channel analysis," Encyclopedia of cryptography and security, Kluwer Academic publishers, pp.571-576, 2005.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proceedings of Advances in cryptology (Crypto ''99), LCNS 1666, pp.388-397, 1999.

저자소개

최 종 석(Jong-Seok Choi) 준회원

- 2004년 3월 ~ 현재 : 동명대학교 정보보호학과 학생

<관심분야> : 암호프로토콜, USN

신 승 수(Seung-Soo Shin) 종신회원

- 1988년 2월 : 충북대학교 수학과(이학사)
- 1993년 2월 : 충북대학교 수학과(이학석사)
- 2001년 2월 : 충북대학교 수학과(이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야> : 암호프로토콜, 무선 PKI, 네트워크 보안, USN