Security Improvement to a Remote User Authentication Scheme for Multi-Server Environment*

Lee, Young Sook · Kim, Jee Yeon · Won, Dong Ho

Multi-Server 환경에서의 사용자 인증 스킴의 안전성 향상

이 영 숙** · 김 지 연*** · 원 동 호****

〈Abstract〉

Recently, Tsai proposed a remote user authentication scheme suited for multi-server environments, in which users can be authenticated using a single password shared with the registration center. Our analysis shows that Tsai et al's scheme does not achieve its fundamental goal of password security. We demonstrate this by mounting an undetectable on-line password guessing attack on Tsai et al.'s scheme.

Key Words : Authentication Scheme, Smart Card, Password, Undetectable On-line Password Guessing Attack, Multi-server Environments

Ⅰ. 서론

Tsai[1] proposed an efficient remote user authentication scheme suited for multi-server environments[1-12]. Multi-sever environments consist of four participant: a registration center, a remote user, and multiple service provider servers. The registration center and all system servers are assumed to be trustworthy. In their article, they claim that the user can be authenticated by all servers included in multi-server environments using a single password shared with the registration center and establishes the session key to be shared with between the server and the user. In addition to making this claim, Tsai claims to exhibit various merits with its scheme: (1) it allows the user to register only once with the registration center and then he/she is able to gain access to all servers included in multi-server environments without registering with every single server; (2) it does not require any server and the registration center to maintain a password table for verifying the legitimacy of login users; (3) it allows users to choose and change their passwords according to their liking and hence gives more user convenience; (4) it does not require synchronized clocks between in the network by using

* 이 논문은 2011년 호원대학교 연구비 지원을 받은 것임.
** 호원대학교 사이버수사 경찰학부 조교수(제1저자)
*** KISA ISMS, PIMS 인증 심사원
**** 성균관대학교 정보통신공학부 교수(교신저자)

random numbers called nonces; (5) it is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations.

However, in this article, we uncover that Tsai's scheme does not guarantee its main security goal of password security. We show this by mounting an undetectable on-line password guessing attack on Tsai's scheme. What we do in this work is to report this security vulnerabilities of Tsai's scheme and to show how to eliminate them.

The remainder of this paper is organized as follows. Section 2 reviews Tsai's remote user authentication scheme. Section 3 presents our attacks on Tsai's scheme and offers a security patch for the scheme. Finally, we conclude this work in Section 4.

II. Review of Tsai's Authentication Scheme

This section reviews a remote user authentication scheme[5, 6, 9, 13-18] proposed by Tsai[1]. The scheme participants include a registration center, a remote user, and multiple service provider servers. For simplicity, we denote the registration center by RC, the remote user by U_i, and the servers by S_1, S_2, ..., S_n. The scheme assumes that the registration center RC is a trust party responsible for securely delivering the secret keys to be shared with between U_i and S_j.

Tsai's scheme consists of four phases: initialization phase, registration phase, login phase, and authentication phase. The initialization phase is processed when the sever who wants to join to the system registers with the registration center. The registration phase is performed only once per user when a new user registers itself with the registration center. The login and the authentication phases are carried out whenever a user wants to gain access to each server included in multi-server environments. Before the registration phase is performed for the first time, the registration center RC decides on the following system parameters: a one-way hash function h and two cryptographic keys x and y. The keys x and y are shared securely with the registration center.

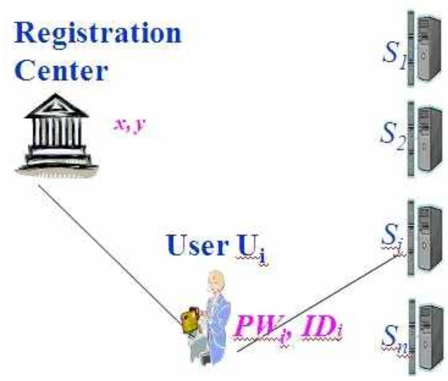

Fig 1. Consist of multi-server environment

2.1 Initialization Phase.

This phase is invoked whenever a server wants to join this group. During this phase, the registration center RC and the server S_j perform the following running:

Step 1. A server S_j who wants to registration with the system submits it's identity SID_j to the registration center RC via a secure channel.

Step 2. After receiving S_j's identity SID_j, RC computes ρ_j as $\rho_j = h(x, SID_j)$ and sends $\langle\rho_j\rangle$ to RC through a secure channel.

2.2 Registration Phase

This is the phase where a new registration of a user takes place. The registration proceeds as follows:

Step 1. A user U_i, who wants to register with the registration center RC, chooses its password PW_i at will and submits a registration request, consisting of its identity ID_i and PW_i, to the registration center RC via a secure channel.

Step 2. Upon receiving the request $\langle ID_i, PW_i \rangle$, RC computes

$Z_i = h(ID_i||x)$

$K_i = Z_i \oplus h(PW_i)$

and issues a smart card containing $\langle K_i, h(\cdot) \rangle$ to U_i.

2.3 Login Phase

When U_i wants to log in to the system, he inserts his smart card into a card reader and enters his identity ID_i and password PW_i. Given ID_i and PW_i, the smart card generates the random nonce N_i and computes

$Z_i = K_i \oplus h(PW_i)$ and $C_1 = Z_i \oplus N_i$.

The smart card then sends the login request message $\langle ID_i, C_1 \rangle$ to the server S_j.

2.4 Authentication Phase

With the login request message $\langle ID_i, C_1 \rangle$, the scheme enters the authentication phase during which S_j, RC, and U_i perform the following steps:

Step 1. When the login request arrives $\langle ID_i, C_1 \rangle$, the server S_j first chooses the random nonce N_{s1} and computes $C_2 = \rho_j \oplus N_{s1}$. Then S_j sends $\langle ID_i, SID_j, C_1, C_2 \rangle$ to the registration center RC.

Step 2. After receiving $\langle ID_i, SID_j, C_1, C_2 \rangle$ from S_j, the registration center generates the random nonce N_{rc} and computes $N'_{s1} = h(SID_j||y) \oplus C_2$ and $C_3 = N_{rc} \oplus h(SID_j||y)$. RC then sends the response message $\langle C_3 \rangle$ to the server S_j.

Step 3. When the server receives C_3, S_j computes $N'_{rc} = C_3 \oplus \rho_j$ and $C_4 = h(\rho_j||N_{s1}) \oplus N'_{rc}$ and sends $\langle C_4 \rangle$ to RC.

Step 4. Having received C_4 from S_j, RC computes

$C'_4 = h(h(SID_j||y)||N'_{s1}) \oplus N_{rc}$

$N'_i = h(ID_i||x) \oplus C$

$C_5 = h(h(SID_j||y)||N'_{s1}||N_{rc})$

$C_6 = h(h(SID_j||y)||N'_{s1}+1||N_{rc}+2) \oplus h(h(ID_i||x)||N'_i)$.

Now RC verifies the correctness of C_4 by checking that C'_4 equals C_4. If correct, RC accepts as the authentic server and sends $\langle C_5, C_6 \rangle$ otherwise, stops executing the scheme.

Step 5. After receiving $\langle C_5, C_6 \rangle$, S_j chooses the random nonce N_{s2} and computes

$C'_5 = h(\rho_j||N_{s1}||N'_{rc})$

$C_7 = C_6 \oplus h(\rho_j||N_{s1}+1||N'_{rc}+2)$

$C_8 = C_1 \oplus C_7$

$V_s = C_7 \oplus N_{s2}$

$C_9 = h(C_7||N_{s2}) \oplus C_8$.

The server S_j checks that C'_5 equals C_5. If they are not equal, S_j believes that he is talking to illegal registration center and aborts the scheme. Otherwise, S_j sends $\langle V_s, C_9 \rangle$ to the user U_i.

Step 6. Upon receiving the message $\langle V_s, C_9 \rangle$, U_i computes

$C'_7 = h(Z_i||N_i)$

$N'_{s2} = C'_7 \oplus V_s$

$D_8 = C'_7 \oplus C_1$

$C'_9 = h(C'_7 || N'_{S2}) \oplus D_8$

$C_{10} = h(C'_7 || D_8 || N'_{S2})$.

Then user U_i verifies that C'_9 equals C_9. If they are equal, U_i believes S_j as authentic and sends the response message $\langle C_{10} \rangle$. Otherwise, U_i aborts its login attempt.

Step 7. After receiving the message $\langle C_{10}, S_j \rangle$ computes $C'_{10} = h(C_7 || C_8 || N_{s2})$ and checks that whether C'_{10} equals C_{10} or not. If the two variables are not equal, S_j rejects the login request. Otherwise, S_j computes the session key $sk = h(C_7 + 1 || C_8 + 2 || N_{s2} + 3)$ which is used to encrypted all following communications between the server S_j and the remoter user U_i.

Ⅲ. Cryptanalysis of Tsai's Scheme

Unfortunately, Tsai's scheme Tsai[1] described above is completely insecure in the presence of an active adversary. To show this, we present an undetectable on-line password guessing attack that exploits password security weaknesses in the scheme.

3.1 Undetectable on-line password guessing attack

An attacker also may try to verify a guessed password in an on-line transaction; he verifies his guess using responses of a server. If his guess fails, he starts a new transaction with the server using another guessed password. However, in successful attack, a failed guess cannot be detected and logged by the server, as the server is not able to distinguish an honest request from a malicious one. In Tasi's protocol, assume that an attacker has stolen the U_i's smart card or gained access to it and extracted the secret values stored in it by monitoring its power consumption[19, 20]. Now the attacker U_a has obtained the value K_i stored in the U_i's smart card. Then the following description represents our undetectable on-line password guessing attack mounted by the attacker U_a against U_i's password: The attacker U_a, who wants to find out PW_i, now guesses possible passwords and checks them for correctness.

1. The attacker U_a, who has obtained K_i stored in its smart card, chooses the random nonce N_a and computes $C_a = K_i \oplus h(PW'_i) \oplus N_a$ using guessed password PW'_i. Then, U_a posing as U_i, sends $\langle ID_i, C_a \rangle$ to the server S_j
2.. After receiving $\langle ID_i, C_a \rangle$, the server S_j computes C_2 and sends the message $\langle ID_i, SID_j, C_a, C_2 \rangle$ to the registration center RC.
3. Since, from RC's point view, ID_i SID_j, C_a, C_2 are indistinguishable from ID_i, SID_j, C_i, C_2 of an honest execution, RC believes that the message $\langle ID_i, C_a \rangle$ is from U_i. Hence, RC operates as specified in protocol using the received messages from S_j. The registration center RC computes C_3 and sends C_3 to the server S_j.
4. After receiving the value of C_3, S_j computes C_4 and sends the value to RC.
5. The received message from S_j will pass the verification test of RC since the computation value C_4 will be successful proceeding the received value from S_j. RC proceeds to compute C_5 and C_6 and sends the message $\langle C_5, C_6 \rangle$.
6. Since C_5 is valid, everything proceeds as usual. In response to U_a's login message, S_j computes

$$C_7 = C_6 \oplus h((\rho_j || N_{s1} + 1 || N'_{rc} + 2)$$
$$C_8 = C_1 \oplus C_7$$
$$V_s = C_7 \oplus N_{m2}$$
$$C_9 = h(C_7 || N_{s_2}) \oplus C_8.$$

Then S_j sends $\langle V_s, C_9\rangle$ to U_a posing as U_i.

7. Now, an attacker U_a upon receiving V_s and C_9 from S_j, computes

$$C'_7 = h(K_i \oplus h(PW'_i)) || N_a)$$
$$N'_{S2} = C'_7 \oplus V_s$$
$$D_8 = C'_7 \oplus C_a$$
$$C'_9 = h(C'_7 || N'_{s2}) \oplus D_8.$$

U_a then verifies the correctness of PW'_i by checking the equality $C'_9 = C_9$. Notice that if PW'_i and PW_i are equal, then $C'_9 = C_9$ ought to be satisfied.

8. U_a repeats a new transaction with the server using another guessed password until a correct password is found.

3.2 Preventing the attack

We now figure out what is wrong with the scheme and how to fix it. The fixed scheme is given mainly to provide a better insight into the failure of Tsai's scheme. Flaws in the scheme The main flaw in Tsai's scheme is that there is no way for the registration center to check whether the received message $\langle C_1\rangle$ is correctly sent or not. The registration center can be sure of is that C_1 is from the legitimate user U_i. This oversight allows the attacker in our attack to send the forged message $\langle ID_i, C_a\rangle$ without being detected by the registration center.

This flaw exploited by the attacker is that the scheme does not provide RC with any proof necessary to verify that C_1 is indeed form U_i. Notice that checking the correctness of $C_9 \stackrel{?}{=} h(K_i \oplus h(PW'_i)|| N_a)|| N'_{s2}) \oplus D_8$ gives no proof that such is the case; for example, by checking the correctness C_9, U_i is assured only that guessed password PW'_i is legitimate user U_i's password. These flaws together allow the adversary to completely compromise the password security of the protocol.

Countermeasure : The simple way to resolve the security problem with Tsai's scheme would be to change the computations of C_1, N'_i, C_6 and C'_7 to:

$$C_1 = (Z_i || SID_j) \oplus N_i$$
$$N'_i = (h(ID_i || x) || SID_j) \oplus C_1$$
$$a = C_1 \oplus N'_i$$
$$a \stackrel{?}{=} h(ID_i || x) || SID_j)$$
$$C_6 = h(h(SID_j || y) || N'_{s1} + 1 || N_{rc} + 2) \oplus h(h(ID_i || x) || SID_j || N'_i)$$
$$C'_7 = h(Z_i || SID_j || N_i).$$

A high level depiction of the scheme is given in Fig. 2 and a more detailed description follows:

In the Table 1, we compare our proposed scheme with previously published Tsai's scheme. It is easy to

Table 1. Comparison of countermeasure between Tsai's scheme and Our proposed scheme

<table>
<tr><th>Tsai's scheme</th><th>Our proposed scheme</th><th>Need for countermeasure</th></tr>
<tr><td>$C_1 = Z_i \oplus N_i$</td><td>$C_1 = (Z_i || SID_j) \oplus N_i$</td><td rowspan="4">To verify "C_1 is indeed from U_i"</td></tr>
<tr><td>$N'_{s1} = h(SID_j || y) \oplus C_2$</td><td>$N'_i = (h(ID_i || x) || SID_j) \oplus C_1$</td></tr>
<tr><td>$C_6 = h(h(SID_j || y) || N'_{s1} + 1 || N_{rc} + 2) \oplus h(h(ID_i || x)$</td><td>$C_6 = h(h(SID_j || y) || N'_{s1} + 1 || N_{rc} + 2) \oplus h(h(ID_i || x) || SID_j || N'_i)$</td></tr>
<tr><td>$C'_7 = h(Z_i || N_i)$</td><td>$C'_7 = h(Z_i || SID_j || N_i)$</td></tr>
</table>

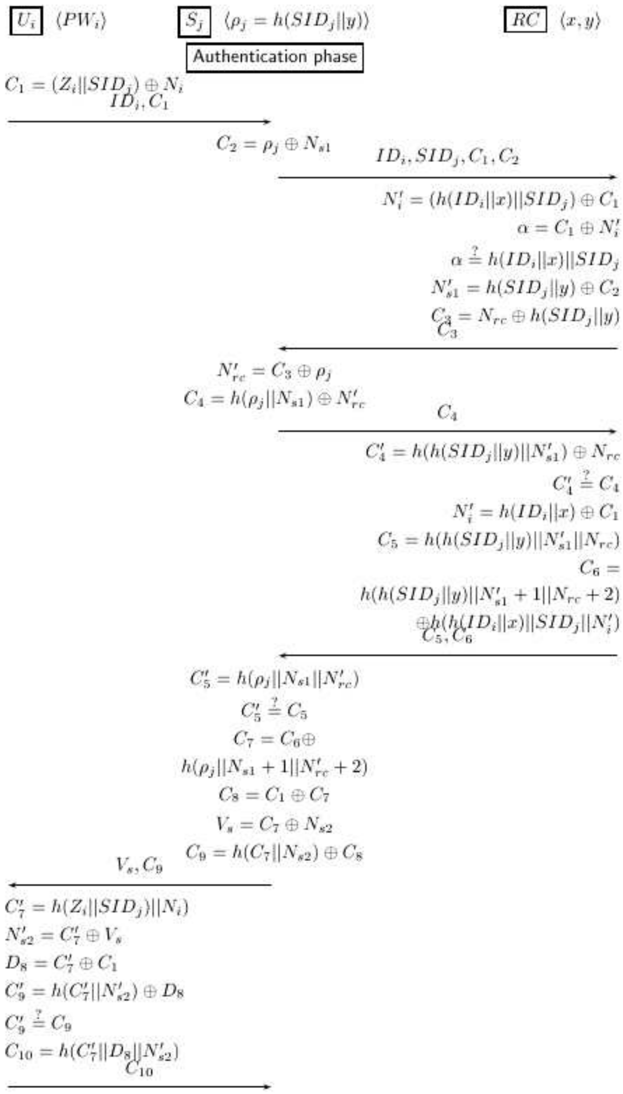

Fig 2. A countermeasure on Tsai's scheme:

see that our proposed authentication scheme can provide *RC* with the proof necessary to verify that C_1 is indeed from U_i.

Ⅳ. Conclusion

This work has considered the security of Tsai's authentication scheme[1] for multi-server environment. We demonstrate this by an undetectable on-line password guessing attack that completely compromises the password security of the scheme. In addition, we have recommended a small change to the scheme that can address the identified security problem.

Reference

[1] Tsai J. -L. Efficient multi-server authentication scheme based on one-way hash function without verification table, Computers & Security 27, 2008, pp.115-121.

[2] Y. Chen, C. -h. Huang, J. -s. Chou, "A Novel multi-server authentication protocol", http://eprint.iacr.org/2009/176, Cryptology ePrint Archive, 2009.

[3] Chang C. and Kuo J. Y. An efficient multi-server password authenticated keys agreement scheme using smart cards with access control, IEEE Proceeding of the 19th International Conference on Advanced Information Networking and Applications 2, 2005, pp.257-260.

[4] Chang C. and Lee J. S., An efficient and secure multi-server password authentication scheme using smart cards, IEEE Proceeding of the International Conference on Cyberworlds, 2004.

[5] Juang W. S. Efficient multi-server password authenticated key agreement using smart cards, IEEE Transaction on Consumer Electronics 50(1), 2004, pp.251-255.

[6] Ku W. -C., Chang S. -T., and Chiang M. -H. Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture, IEICE Transactions on Communications E88-B(8), 2005, pp.3451-3454.

[7] Li L. -H., Lin I. -C., and Hwang M. -S. A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transaction on Neural Networks 12(6), 2001, pp. 1498-1504.

[8] Lin I. -C., Hwang M. -S., and Li L. -H. A new remote user authentication scheme for multi-server internet environments, Future Generation Computer System 19, 2003, pp.13-22.

[9] Sun H. -M. An efficient remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 46(4), 2000 pp.958-961.

[10] Tsuar W. -J. An enhanced user authentication scheme for multi-server internet services, Applied Mathematics and Computation 170, 2005, pp.258-266.

[11] Tsuar W. -J., Wu C. -C., and Lee W. -B. A flexible user authentication for multi-server internet services, Networking-JCN 2001 LNCS 2093, 2001, pp.174-183.

[12] Tsuar W. -J., Wu C. -C., and Lee W. -B. A smart card-based remote scheme for password authentication in multi-server Internet services, Computer Standards & Interfaces 27, 2004, pp.39-51.

[13] Chang C. -C. and T. -C. Wu Remote password authentication with smart cards, IEE Proceedings E -Computers and Digital Techniques 138(3), 1991, pp. 165-168.

[14] Chien H. -Y., Jan J. -K., and Tseng Y. -M. An efficient and practical solution to remote authentication: smart card, Computers & Security 21(4), 2002, pp.372-375.

[15] Hsu C. -L. Security of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards and Interfaces 26(3), 2004,

pp. 167-169.

[16] Hwang M. -S. and Li L. -H. A new remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 46(1), 2000, pp. 28-30.

[17] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in Advances in Cryptology-CRYPTO99, 1999, pp.388-397.

[18] M. Kim, K. Lee, S. Kim, D. Won, Efficient and Secure Authentication Scheme Preserving User Anonymity, The Korea-Society of Digital Industry& Information Management, 2010, 6(3), pp.69-77.

[19] T. S. Messergers, E. A. Dabbish, R. H. Sloan, Examining smart card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5), 2002, pp.541-552.

[20] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in Advances in Cryptology{CRYPTO 99}, 1999, pp.388-397.

■ 저자소개 ■

이 영 숙
Lee, Young Sook

2009년 3월~현재
호원대학교 사이버수사경찰학부 조교수
2011년 7월 ~현재
호원대학교 사이버수사경찰학부 학부장
2010년 1월~2011년 6월
호원대학교 기획조정처 경영평가실장
2008년 8월 성균관대학교 컴퓨터공학과 (공학박사)
2005년 2월 성균관대학교 정보보호학과 (공학석사)
1987년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론, 네트워크 보안, 스마트폰 보안
E-mail : ysooklee@howon.ac.kr

김 지 연
Kim, Jee Yeon

2007년 9월~현재
KISA ISMS, PIMS 인증 심사원
1996년 12월~2007년 1월
한국정보보호진흥원 선임연구원
2006년 2월 성균관대학교 전기전자및컴퓨터공학과(공학박사)
2007년 2월 성균관대학교 정보공학과(공학석사)
1995년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론, 정보보호관리체계 인증
E-mail : jeeyeonkim@paran.com

원 동 호
Won, Dong Ho

현재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장
2002년~2008년
대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
2002년~2003년
한국정보보호학회장
1996년~1998년
국무총리실 정보화추진위원회 자문위원
1988년~2003년
성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1985년~1986년
일본 동경공업대 객원연구원
1978년~1980년
한국전자통신연구원 전임연구원
1976년~1988년
성균관대학교 전자공학과(학사, 석사, 박사)

관심분야 : 암호이론, 정보이론, 정보보호
E-mail : dhwon@security.re.kr

논문접수일 : 2011년 8월 20일
수 정 일 : 2011년 10월 04일
게재확정일 : 2011년 10월 20일