http://dx.doi.org/10.7236/JIIBC.2013.13.1.273
JIIBC 2013-1-37

멀티서버를 위한 안전한 동적 ID 기반 원격 사용자 인증 방식에 대한 안전성 분석

Security Analysis of a Secure Dynamic ID based Remote User Authentication Scheme for Multi-server Environment

양형규*

Hyung-Kyu Yang

요 약 최근에, 멀티서버 환경을 위한 스마트 카드를 이용한 사용자 인증 방식이 실질적인 응용 분야에서 적용되고 있다. 2009년도에 Liao-Wang은 멀티서버를 위한 안전한 동적 ID 기반 원격 사용자 인증 방식을 제안하였다. 이 방식은 여러 종류의 가능한 공격에 안전하면서 사용자 익명성 보장하였다. 본 논문에서 우리는 Liao-Wang의 방식에 대한 안정성을 분석하고, Liao-Wang의 방식이 위조 공격, 패스워트 추측 공격, 세션키 공격 그리고 내부자 공격에 취약하다는 것을 보여준다. 추가로 Liao-Wang의 방식이 사용자와 서버간의 사용자 익명성 역시 제공하지 못한다는 것을 증명한다.

Abstract Recently, user authentication schemes using smart cards for multi-server environment have been proposed for practical applications. In 2009, Liao-Wang proposed a secure dynamic ID based remote user authentication scheme for multi-server environment that can withstand the various possible attacks and provide user anonymity. In this paper, we analyze the security of Liao-Wang's scheme, and we show that Liao-Wang's scheme is still insecure against the forgery attack, the password guessing attack, the session key attack, and the insider attack. In addition, Liao-Wang's scheme does not provide user anonymity between the user and the server.

Key Words : Smart card, User authentication, forgery attack, user anonymity, session key attack

Ⅰ. Introduction

With the rapid development of internet technology, user authentication scheme in e-commerce has been becoming one of important security issues. However, the security weaknesses in the remote user authentication scheme have been exposed seriously due to the careless password management and the sophisticated attack techniques.

If conventional password-based authentication scheme is applied to multi-server environment, each remote user has to login to various servers repetitively and remember many sets of identity/password. It is inefficient and is not secure the authentication scheme

*정회원, 강남대학교 컴퓨터미디어정보공학부
접수일자 : 2013년 1월 20일, 수정완료 : 2013년 2월 7일
게재확정일자 : 2013년 2월 8일

Received: 20 January 2013 / Revised: 7 February 2013 / Accepted: 8 February 2013
*Corresponding Author: hkyang@kangnam.ac.kr
Dept. of Computer Engineering, Kangnam University, Korea

from compromise of the identity and password. Several authentication schemes for multi-server environment have been proposed to improve the security and efficiency[1-9]. In general, a secure and efficient remote user authentication scheme for multi-server environment usually should provide the following basic criteria: single registration, low computation, no verification table, update password securely and freely, mutual authentication, session key agreement, and security.

In 2003, Lin et al. proposed a new remote user authentication scheme for multi-server architecture[2]. However, Juang in 2004 pointed out that Lin et al.'s scheme is not enough efficient for authentication process, and then proposed an efficient multi-server password authenticated key agreement using smart cards[3]. In 2007, Hwang and Shiau showed Juang's scheme lacks of explicit key authentication and is inefficient with respect to communication costs, and then they proposed provably efficient authenticated key agreement protocol for multi-server[5]. However, their scheme still does not provide forward secrecy. Recently, in 2009, Liao-Wang proposed a secure dynamic ID based remote user authentication scheme for multi-server environment, and they claimed that can withstand the various possible attacks and provide user anonymity[7].

In this paper, we analyze the security of Liao-Wang's scheme. And we show that Liao-Wang's scheme is still insecure against the various known attacks and does not provide user anonymity. To analyze the security, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption and intercept messages communicating between the user and the server[8-10].

This paper is organized as follows. In section 2, we briefly review Liao-Wang's scheme. In section 3, we describe the security analysis of Liao-Wang's scheme. Finally, conclusions are presented in section 4.

II. Reviews of Liao-Wang's Scheme

In 2009, Liao-Wang proposed a secure dynamic ID based remote user authentication scheme for multi-server environment. This scheme is composed of four phases: registration phase, login phase, mutual verification and session key agreement phase, and password change phase. The notations used in this paper are listed in Table 1.

표 1. 용어 표기 및 정의
Table 1. Notation and Definition

Notation	Description
U_i	User i
RC	Registration center
S_j	Server j
PW_i	Password of the user i
ID_i	Identification of the user i
SID_j	Identification of the server j
h()	A one-way hash function
x	A master secret key of the registration center
y	A secret number shared with the registration center and all servers
N_i	A random number chosen by the user
N_j	A random number chosen by the server
$A \| B$	A concatenates with B
$A \oplus B$	A exclusive-OR B

1. Registration Phase

This phase works whenever a user wants to register in the multi-server system. The user U_i submits his identity ID_i and password PW_i to the registration center RC via a secure channel. Then the registration center performs the following steps.

R1. The registration center computes $T_i=h(ID_i \| x)$, $V_i=T_i \oplus h(ID_i \| PW_i)$, $B_i= h(PW_i) \oplus h(x)$ and $H_i=h(T_i)$.

R2. The registration center issues the smart card with the secret values $(V_i,B_i,H_i,h(),y)$ to the user via a secure channel.

2. Login Phase

This phase works whenever a user wants to login to the remote server. The user U_i inserts his smartcart to the card reader and keys his identity ID_i, password PW_i and the server identity SID_i. Then the smart card performs the following steps. The login and authentication phase are illustrated in Fig. 1.

L1. The smart card computes $T_i*=V_i \oplus h(ID_i \| PW_i)$, and then checks whether the computed value $h(T_i^*)$ equals H_i stored in the smartcard or not. If it holds, the smartcard performs the next steps.

L2. The smart card generates random nonce N_i and computes $CID_i=h(PW_i) \oplus h(T_i* \| y \| N_i)$, $P_{ij}=T_i* \oplus h(y \| N_i \| SID_j)$ and $Q_i=h(B_i \| y \| N_i)$.

L3. The smart card sends the login request message $\{CID_i, P_{ij}, Q_i, N_i\}$ to the server S_j.

3. Mutual Verification and session key agreement phase

After receiving the login request message, the server S_j and the user U_i authenticate each other and agree on a session key SK such as the following steps.

M1. The server computes $T_i^*=P_{ij} \oplus h(y \| N_i \| SID_j)$, $h^*(PW_i)=CID_i \oplus h(T_i* \| y \| N_i)$ and $B_i^*= h^*(PW_i) \oplus h(x)$.

M2. The server checks whether the computed value $h(B_i^* \| y \| N_i)$ equals Q_i or not. If it holds, the server performs the next steps.

M3. The server generates random nonce N_j and computes $M_{ij1}=h(B_i^* \| y \| N_i \| SID_j)$, and then sends back the reply message $\{M_{ij1},N_i\}$ to the user.

M4. After receiving the reply message, the user checks whether the computed value $h(B_i \| y \| N_i \| SID_j)$ equals Mij1 or not. If it holds, the user performs the next steps.

M5. The smart card computes $Mij2=h(B_i \| y \| N_j \| SID_j)$, and then sends back the message { Mij2} to the server.

M6. After receiving the message, the server checks whether the computed value $h(B_i^* \| y \| N_j \| SID_j)$ equals Mij2 or not. If it holds, the user is authenticated by the server.

M7. After completing the mutual authentication, the user and the server compute their session key respectively such as $SK=h(B_i \| N_i \| N_j \| y \| SID_j)$.

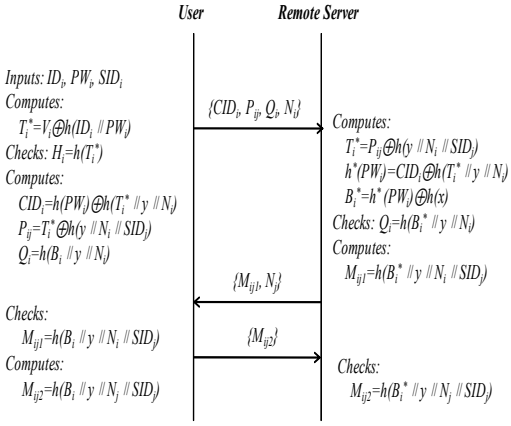

그림 1. Liao-Wang 방식의 인증 프로토콜
Fig. 1. Authentication Protocol of Liao-Wang's Scheme

4. Password Change Phase

This phase works whenever a user wants to update his password without the help of the registration center. The user inserts his smart cart to the card reader, and keys his identity ID_i and password PW_i. Then the user performs the following steps.

P1. The smart card works as the step 1 of login phase for assuring the legality of the cardholder and allows the cardholder to resubmit a new password PW_i^{new}.

P2. The smart card computes $V_i^{new}=T_i \oplus h(ID_i \| PW_i^{new})$ and $B_i^{new}=B_i \oplus h(PW_i) \oplus h(PW_i^{new})$.

P3. Then, the smart card updates with V_i^{new} and B_i^{new} instead of V_i and B_i each other.

Ⅲ. Security Analysis of Liao-Wang's Scheme

To analyze the security of Liao-Wang's scheme, we assume that an attacker could obtain the secret values (B_i,y) stored in the smart card by monitoring the power consumption and intercept messages (P_{ij}, N_i,N_j) communicating between the user and the server[8-9].

1. Forgery Attack

With the extracted secret values, an attacker can easily perform the user impersonation attack as the following steps. The procedure of the user impersonation attack is illustrated in Fig.2.

FA1. The attacker computes easily $T_i^*=P_{ij}\oplus h(y \| N_i \| SID_j)$, $h^*(PW_i)=CID_i\oplus h(T_i* \| y \| N_i)$ and $B_i^*=h^*(PW_i)\oplus h(x)$.

FA2. Then, the attacker computes the following equations, where N_i^* is a random number chosen by the attacker.

$CID_i*=h(PW_i)\oplus h(T_i* \| y \| N_i*)$

$P_{ij}^*=T_i*\oplus h(y \| N_i* \| SID_j)$

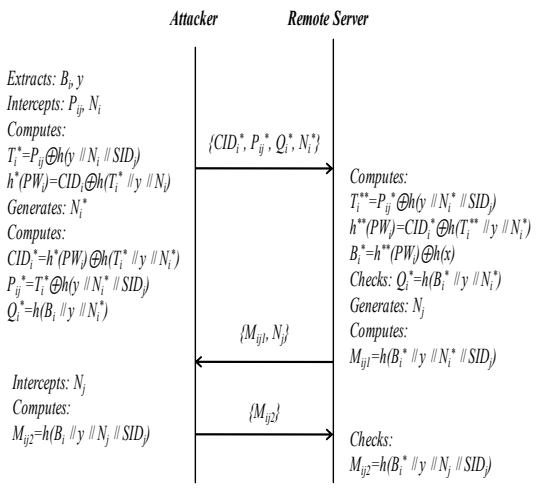

그림 2. 사용자 위장 공격
Fig. 2. User Impersonation Attack.

$Q_i^*=h(B_i \| y \| N_i*)$

FA3. The attacker sends the forged login request message $\{CID_i^*, P_{ij}^*,Q_i^*, N_i*\}$ to the remote server S_j.

FA4. Upon receiving the forged message, S_i computes $T_i^{**}=P_{ij}^*\oplus h(y \| N_i* \| SID_j)$, $h^{**}(PW_i)= CID_i*\oplus h(T_i** \| y \| N_i*)$ and $B_i^*=h^{**}(PW_i)\oplus h(x)$.

FA5. Then, S_i checks whether the computed value $h(B_i^* \| y \| N_i*)$ equals Q_i^* or not. If it holds, the server performs the next steps.

FA6. S_i generates random nonce N_j and computes $M_{ij1}=h(B_i^* \| y \| N_i* \| SID_j)$, and then sends back the reply message $\{M_{ij1},N_j\}$ to the user.

FA7. After receiving the reply message, the attacker computes $M_{ij2}^*=h(B_i \| y \| N_j \| SID_j)$, and then sends the forged message $\{M_{ij2}^*\}$ to the server.

FA8. After receiving the message, the server checks whether the computed value $h(B_i^* \| y \| N_j \| SID_j)$ equals M_{ij2}^* or not. If it holds, the attacker is authenticated as the legal user by the server.

Also, with the extracted secret values (B_i, y) and the intercepted massage (N_i), the attacker can perform the server masquerading attack by computing $M_{ij1}^*=h(B_i \| y \| N_i \| SID_j)$ and sending the reply message $\{Mij1^*,N_i^*\}$ to the user, where N_j* is a random number chosen by the attacker. After receiving the reply message from the attacker, the user checks whether the computed value $h(B_i \| y \| N_i \| SID_j)$ equals M_{ij1}^* or not. If it holds, the user can authenticate the attacker as the legal server.

2. Session Key Attack

After mutual authentication is performed, the legal user and the remote server can use the session key SK in the public channel to encrypt/decrypt all the messages. In Liao-Wang's scheme, the attacker can establish the one-time session key $SK=h(B_i \| N_i \| N_j \| y \| SID_j)$ as shown in the session key agreement phase if the attacker can obtain the secret values (B_i, y) stored in the smart card and intercept messages (N_i, N_j) communicating between the server and the user. Thus, we can see that the Liao-Wang's scheme does

not provide the session key agreement.

3. Password Guessing Attack

With the extracted secret values (B_i, y) stored in the smart card card and the intercepted messages $\{M_2, M_3\}$ communicating between the user and the server, the attacker can easily find out legal user's password PW_i in which each guess PW_i^* for PW_i.

PA1. The attacker can compute $h(PW_i^*)=CID_i \oplus h(P_{ij} \oplus (h(y \| N_i \| SID_j) \| y \| N_i)$ in the login phase.

PA2. The attacker verifies the correctness of user's password PW_i^*.

PA3. The attacker repeats the above steps by replacing another guessed password PW_i^* until the correct password PW_i is found.

Thus, the attacker can perform the off-line password guessing attack, and can successfully impersonate the legal user with the guessed user password.

4. Insider Attack

In the registration phase, if the user's password PW_i is revealed to the server, the insider of the server may directly obtain the user's password. With these secret information, the insider as an attacker can impersonate as the legal user to access the user's other accounts in other server if the user uses the same password for the other accounts.

Ⅳ. Conclusion

Liao-Wang, in 2009, proposed a secure dynamic ID based remote user authentication scheme for multi-server environment and they claimed that can withstand the various possible attacks and provide mutual authentication. In this paper, we analyzed the security of Liao-Wang's scheme. And we showed that Liao-Wang's scheme is not secure against the user impersonation attack, the server masquerading attack, the off-line password guessing attack and insider attack. In addition, we can see that Liao-Wang's scheme fails to provide mutual authentication and session key agreement

참 고 문 헌

[1] K. Choi, T. Kim, S. Yeo, E. Cho, "A Study on the Network Security Level Management", Journal of Korean Institute of Information Technology, vol. 7, issue 1, pp. 214-219, Feb 2009.

[2] Lin, I.C., Hwang, M.S., Li, L.H, "A New Remote User Authentication Scheme for Multi-server Architecture". Future Generation Computer System, vol. 19, pp. 13-22, 2003

[3] Juang, W.S, "Efficient Multi-server Password Authenticated Key Agreement using Smart Cards". IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251-255, 2004.

[4] Chang, C., 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] Hwang, R.J., Shiau, S.H, "Provably Efficient Authenticated Key Agreement Protocol for Multi-servers". The Computer Journal, vol. 50, no. 5, pp. 602-615, 2007.

[6] Tsai, J.L, "Efficient Multi-server Authentication Scheme based on One-way Hash Function without Verification Table", Computer and Security, vol. 27, pp. 115-121, 2008.

[7] Liao, Y.P., Wang, S.S, "A Secure Dynamic ID based Remote User Authentication Scheme for Multi-server Environment", Computer Standards and Interfaces, vol. 31, pp. 24-29, 2009.

[8] Kocher, P., Jaffe, J., Jun, B, "Differential Power Analysis", Proceedings of Advances in Cryptology, pp. 388-397, 1999

[9] Messerges, T.S., Dabbish, E.A., Sloan, R.H,

"Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Transactions on Computers 51(5), pp. 541-552, 2002.

[10] Y. Kim, Y. Jeong, G. Park, "An Authentication Protocol Proposal to Guarantee Reliability of Wireless Node in IEEE 802.16s", Journal of Korean Institute of Information Technology, vol. 6, issue 4, pp. 87-93, Aug 2008.

※ 본 연구는 2011년 강남대학교 교내연구비 지원 연구임.

저자 소개

양 형 규(정회원)

- 1995년 2월 : 성균관대학교 석사
- 1995년 2월 : 성균관대학교 정보공학과 공학박사
- 1995년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수
- 1984년 12월 ~ 1990년 2월 : 삼성전자 컴퓨터부문 선임연구원

<주관심분야 : 정보보안, 네트워크 보안, DRM>