http://dx.doi.org/10.7236/JIWIT.2012.12.1.231
JIWIT 2012-1-30

스마트 카드를 이용한 생체인식 기반 원격 사용자 인증 스킴의 보안성 개선

Security Enhancement of Biometrics-based Remote User Authentication Scheme Using Smart Cards

안영화*, 주영도**

Young-Hwa An, Young-Do Joo

요 약 2011년에 Das는 Li-Hwang의 스킴의 보안 문제점을 개선하면서 강력한 인증과 상호 인증을 제공할 수 있는 효율적인 생체인식 기반 원격사용자 스킴을 제안하였다. 본 논문에서는 Das의 인증 스킴이 여러 가지 공격들에 대해 안전하지 않으며 상호 인증도 제공하고 있지 않음을 증명하였다. 또한, 본 논문에서는 비록 스마트 카드에 저장되어 있는 비밀정보가 누출된다 하더라도 이와 같은 보안 문제점들을 해결할 수 있는 개선된 스킴을 제안하였다. 보안성 분석 결과, 개선된 스킴은 사용자 위장 공격, 서버 위장 공격, off-line 패스워드 추측 공격 그리고 내부자 공격에 안전하고 사용자와 서버 사이에 상호인증을 제공함을 알 수 있다.

Abstract In 2011, Das proposed an effective biometrics-based remote user authentication scheme using smart cards that can provide strong authentication and mutual authentication, while eliminating the security drawbacks of Li-Hwang's scheme. In this paper, we have shown that Das's scheme is still insecure against several attacks and does not provide mutual authentication. Also, we proposed the enhanced scheme to overcome these security weaknesses, even if the secret information stored in the smart card is revealed. As a result of security analysis, the enhanced scheme is secure against user impersonation attack, server masquerading attack, off-line password guessing attack, and insider attack. And we can see that the enhanced scheme provides mutual authentication between the user and the server.

Key Words : Authentication, User Impersonation Attack, Server Masquerading Attack, Mutual Authentication

Ⅰ. Introduction

With the rapid development of network technology, user authentication scheme in e-commerce and m-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. Several schemes[1-5] have been proposed to improve security, reliability, and efficiency.

In traditional identity-based remote user

*정회원, 강남대학교 컴퓨터미디어공학부
**정회원, 강남대학교 컴퓨터미디어공학부
접수일자 2012.1.8, 수정일자 2012.2.3
게재확정일자 2012.2.10

Received: 8 January 2012 / Revised: 3 February 2012 / Accepted: 10 February 2012
*Corresponding Author: yhan@kangnam.ac.kr
Dept. of Computer and Media Engineering, Kangnam University, Korea

authentications, the security of the remote user authentication is based on the passwords, but simple passwords are easy to break by simply dictionary attacks. Furthermore, both passwords and cryptographic keys are unable to provide non-repudiation because they can be forgotten, lost. Therefore, several biometrics-based remote user authentication schemes[6-10] have been designed to resolve the single password authentication problems. Compared with the traditional password authentication, biometrics-based remote user authentication is inherently more secure and reliable, and it can withstand even professional attacks. There are some advantages of using biometrics key (e.g. fingerprints, faces, irises, hand geometry, and palm-prints etc.) as compared to traditional passwords.

- Biometric keys cannot be lost or forgotten.
- Biometric keys are very difficult to copy or share.
- Biometric keys are extremely hard to forge or distribute.
- Biometric keys cannot be guessed easily.
- Someone's biometrics is not easy to break than others.

In 2010, Li-Hwang[9] proposed an efficient biometrics -based remote user authentication scheme using smart cards. They claimed that their scheme not only keeps good properties (e.g. without synchronized clock, freely changes password, low computational costs, mutual authentication) but also provides non-repudiation. But Das[10] in 2011 pointed out that Li-Hwang's scheme does not resolve flaws in login and authentication, flaws in password change phase, and flaws in verification of biometrics. Then, Das proposed more efficient biometrics-based remote user authentication scheme using smart cards which is secure against the user impersonation attack, the server masquerading attack, the parallel session attack, the stolen password attack, etc. and provide mutual authentication.

In this paper, we analyze the security weaknesses of Das's scheme and we have shown that Das's scheme is still vulnerable to some attacks. In addition, we show that Das's scheme does not provide mutual authentication between the user and the server. To analyze the security analysis of Das's scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption[11-12] and intercept messages communicating between the user and the server.

This paper is organized as follows. In section II, we briefly review Das's scheme. In section III, we describe security weaknesses of Das's scheme. The enhanced scheme and security analysis are presented in section IV, and the conclusions are given in section V.

II. Reviews of Das's Scheme

In 2011, Das[10] proposed an improved biometrics-based remote user authentication scheme using smart cards. This scheme is composed of three phases: registration phase, login phase, and authentication phase. The notations used in this paper are as follows:

표 1. 표기법
Table 1. Notations

Notation	Description
C_i	User i
R_i	Trusted registration centre i
S_i	Server i
PW_i	Password of the user i
ID_i	Identity of the user i
B_i	Biometrics template of the user i
h()	A secure hash function
X_s	A secret information kept by the server
R_c	A random number chosen by the user
R_s	A random number chosen by the server
A ‖ B	A concatenates with B
A⊕B	XOR operation of A and B

1. Registration Phase

Before logging in the remote server, a user C_i initially has to register to the trusted registration centre R_i as the following steps.

1) C_i submits his identifier ID_i and password PW_i to R_i through a secure channel. Also the user inputs his biometrics B_i on the specific device to R_i.
2) R_i computes $f_i=h(B_i)$, $r_i=h(PW_i)\oplus f_i$ and $e_i=h(ID_i \| X_s)\oplus r_i$, where X_s is a secret value generated by the server.
3) R_i stores $(ID_i, h(), f_i, e_i, r_i)$ on the user's smart card and sends it to the user via a secure channel.

2. Login Phase

When the user C_i wants to login the remote server S_i, the user has to perform the following steps.

1) C_i inserts his smart card into a card reader and inputs the personal biometrics B_i on the specific device to verify the user's biometrics. If the biometrics information matches the template stored in system, C_i passes the biometrics verification.
2) C_i inputs the ID_i and PW_i, and then the smart card computes $r_i'=h(PW_i)\oplus f_i$. If $r_i'=r_i$, the smart card computes $M_1=e_i\oplus r_i'$, $M_2=M_1\oplus R_c$, $M_3=h(R_c)$, where R_c is a random number generated by the user.
3) Finally, C_i sends the message $\{ID_i, M_2, M_3\}$ to S_i.

3. Authentication Phase

After receiving the request login message, S_i has to perform the following steps with C_i to authenticate each other.

1) S_i checks the format of ID_i.
2) If the ID_i is valid, S_i computes $M_4=h(ID_i \| X_s)$, $M_5=M_2\oplus M_4$ and verifies whether $M_3=h(M_5)$ or not. If they are equal, S_i computes $M_6=M_4\oplus R_s$, $M_7=h(M_2 \| M_5)$, $M_8=h(R_s)$, where R_s is a random number generated by the server.
3) Then S_i sends the message $\{M_6, M_7, M_8\}$ to C_i.
4) After receiving the message, C_i verifies whether $M_7=h(M_2 \| R_c)$ or not. If they are equal, C_i computes $M_9=M_6\oplus M_1$ and verifies whether $M_8=h(M_9)$ or not.
5) If they are equal, C_i computes $M_{10}=h(M_6 \| M_9)$ and sends the message $\{M_{10}\}$ to S_i.
6) After receiving the message, S_i verifies whether $M_{10}=h(M_6 \| R_s)$ or not. If they are equal, S_i accepts the user's login request.

Ⅲ. Security Weakness of Das's Scheme

In this section, we will analyze the security weaknesses in Das's scheme, biometrics-based remote user authentication scheme. To analyze the security weaknesses, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption[11-12] and intercept messages communicating between the user and the server. Under this assumption, we will discuss several attacks, such as the user impersonation attack, the server masquerading attack, the off-line password guessing attack, and the mutual authentication between the user and the server.

1. User Impersonation Attack

As described the above, the attacker can extract the secret values (e_i, r_i) from the user's smart card illegally by some means and intercept the message $\{ID_i, M_2, M_3\}$ in the login phase. The procedure of the user impersonation attack with the secret values is as the following steps. And the user impersonation attack is illustrated in Fig.1.

1) The attacker computes easily $M_{a1}=e_i\oplus r_i$, $M_{a2}=M_{a1}\oplus R_{ac}$ and $M_{a3}=h(R_{ac})$, where R_{ac} is a random number generated by the attacker.
2) Then, the attacker sends the forged message $\{ID_i, M_{a2}, M_{a3}\}$ to the remote server S_i.
3) Upon receiving the forged message, S_i checks the format of ID_i. If it holds, S_i computes $M_4=h(ID_i \| X_s)$, $M_5=M_{a2}\oplus M_4$ and verifies whether $M_{a3}=h(M_5)$ or not. If they are equal, S_i will be convinced the message $\{ID_i, M_{a2}, M_{a3}\}$ sent from the legitimate

user. Then, S_i makes the reply massage $\{M_6, M_7, M_8\}$ by computing $M_6=M_4 \oplus R_s$, $M_7=h(M_{a2} \| M_5)$, $M_8=h(R_s)$ in the authentication phase.

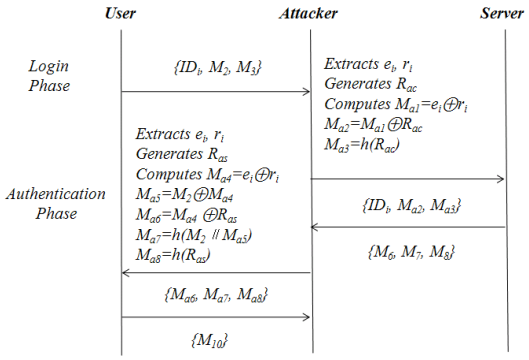

그림 1. 사용자 위장 공격 및 서버 위장 공격
Fig. 1. User Impersonation Attack and Server Masquerading Attack

2. Server Masquerading Attack

As described the above, the attacker can extract the secret values (e_i, r_i) from the user's smart card illegally by some means and intercept the message $\{M_2\}$ in the login phase, $\{M_6, M_7, M_8\}$ in the authentication phase. The procedure of the server masquerading attack with the secret values is as the following steps. And the server masquerading attack is illustrated in Fig.1.

1) The attacker computes easily $M_{a4}=e_i \oplus r_i$, $M_{a5}=M_2 \oplus M_{a4}$, $M_{a6}=M_{a4} \oplus R_{as}$, $M_{a7}=h(M_2 \| M_{a5})$, $M_{a8}=h(R_{as})$, where R_{as} is a random number generated by the attacker.
2) Then, the attacker sends the forged message $\{M_{a6}, M_{a7}, M_{a8}\}$ to the user C_i.
3) Upon receiving the forged message, C_i checks whether $M_{a7}=h(M_2 \| R_c)$ or not. If they are equal, C_i computes and $M_9=M_{a6} \oplus M_1$ and verifies whether $M_{a8}=h(M_9)$ or not. If it holds, C_i will be convinced the message $\{M_{a6}, M_{a7}, M_{a8}\}$ sent from the legitimate server. Then, C_i makes the reply massage $\{M_{10}\}$ by computing $M_{10}=h(M_{a6} \| M_9)$ in the authentication phase.

3. Password Guessing Attack

We assume that an attacker can extract the secret values (r_i, f_i) from the legitimate user's smart card by some means. With these secret values, the attacker can easily find out PW_i by performing the off-line password guessing attack, in which each guess PW_i^* for PW_i can be verified by the following steps.

1) The attacker computes the secret parameter $r_i^*=h(PW_i^*) \oplus f_i$ from the registration phase.
2) The attacker verifies the correctness of PW_i^* by checking $r_i=r_i^*$.
3) The attacker repeats the above steps until a 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. Mutual Authentication

Generally, if an authentication scheme is insecure against user impersonation attack, server masquerading attack, the authentication schemes cannot provide mutual authentication between the user and the remote server. Thus, Das's scheme fails to provide mutual authentication as described the above subsection. Namely, if the attacker can extract the secret values (e_i, r_i) from the legitimate user's smart card illegally by some means and intercept the messages communicating between the user and the server, the attacker can make the modified message easily by computing $M_{a1}=e_i \oplus r_i$, $M_{a2}=M_{a1} \oplus R_{ac}$ and $M_{a3}=h(R_{ac})$ in the login phase. Also, the attacker can make the modified message easily by computing $M_{a6}=M_{a4} \oplus R_{as}$, $M_{a7}=h(M_2 \| M_{a5})$, $M_{a8}=h(R_{as})$. Hence, we can see that Das's scheme fails to provide mutual authentication between the user and the server.

Ⅳ. The Enhanced Scheme and Security Analysis

In this section, we propose an enhanced Das's scheme which can withstand the various attacks with

providing mutual authentication.

1. The Enhanced Scheme

The proposed scheme is divided into three phases: registration phase, login phase and authentication phase. The login and authentication phase are illustrated in Fig. 2.

■ Registration Phase

Before logging in the remote server, a user C_i initially has to register to the trusted registration centre R_i as the following steps.

1) C_i submits his identifier ID_i and password information ($PW_i \oplus K$) to R_i through a secure channel. Also the user submits his biometrics information ($B_i \oplus K$) via the specific device to R_i.
2) R_i computes $f_i=h(B_i \oplus K)$, $r_i=h(PW_i \oplus K) \oplus f_i$ and $e_i=h(ID_i \| X_s) \oplus r_i$, where X_s is a secret value generated by the server and K is a random number generated by C_i.
3) R_i stores (ID_i, h(), f_i, e_i) on the user's smart card and sends it to the user via a secure channel. And C_i stores random number K into the smart card issued by R_i.

■ Login Phase

When the user C_i wants to login the remote server S_i, the user has to perform the following steps.

1) C_i inserts his smart card into a card reader and inputs personal biometrics B_i on the specific device to verify user's biometrics. If the biometrics information matches the template stored in system, C_i passes the biometrics verification.
2) C_i inputs the ID_i and PW_i, and then the smart card computes:

$r_i'=h(PW_i \oplus K) \oplus f_i$
$M_1=e_i \oplus r_i'$
$M_2=M_1 \oplus R_c$
$M_3=h(M_1 \| R_c)$

where R_c is a random number generated by the user.

3) C_i sends the login request message $\{ID_i, M_2, M_3\}$ to S_i.

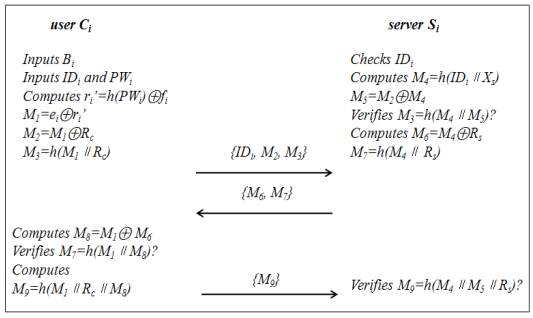

그림 2. 개선된 스킴의 로그인 단계 및 인증 단계
Fig. 2. Login Phase and Authentication Phase of the Enhanced Scheme

■ Authentication Phase

After receiving the request login message, S_i has to perform the following steps with C_i to authenticate each other.

1) S_i checks the format of ID_i.
2) If the ID_i is valid, S_i computes $M_4=h(ID_i \| X_s)$, $M_5=M_2 \oplus M_4$.
3) S_i verifies whether $M_3=h(M_4 \| M_5)$ or not. If they are equal, S_i computes:

$M_6=M_4 \oplus R_s$
$M_7=h(M_4 \| R_s)$

where R_s is a random number generated by the server.

4) Then S_i sends the message $\{M_6, M_7\}$ to C_i.
5) After receiving the reply message, C_i computes $M_8=M_6 \oplus M_1$ and verifies whether $M_7=h(M_1 \| M_8)$ or not. If they are equal, C_i computes $M_9=h(M_1 \| R_c \| M_8)$. Then C_i sends the message $\{M_9\}$ for authentication to S_i.
6) After receiving the message, S_i verifies whether $M_9=h(M_4 \| M_5 \| R_s)$ or not. If they are equal, S_i accepts the user's login request.

2. Security Analysis of the Enhanced Scheme

In this section, we will provide the security analysis of the enhanced scheme based on secure one-way hash function. To analyze the security, we assume that an attacker can extract the secret values (f_i, e_i) from the legitimate user's smart card[11-12].

■ User Impersonation Attack

To impersonate as the legitimate user, an attacker attempts to make a forged login request message which can be authenticated to the server. However, the attacker cannot impersonate the user by forging the login request massage if the attacker can extract the secret values (f_i, e_i) stored in the user's smart card, because the attacker cannot compute the message (M_2, M_3) sending to the server without knowing the secret value X_s kept by the server. Hence, the attacker has no chance to login by launching user impersonation attack.

■ Server Masquerading Attack

To masquerade as the legitimate server, an attacker attempts to make the forged reply massage which can be masqueraded to the user when receiving the user's login request message. However, the attacker cannot masquerade as the server by forging the reply massage, because the attacker cannot compute (M_6, M_7) sending to the user without knowing the secret value X_s kept by the server. Hence, the attacker cannot masquerade as the legitimate server to the user by launching server masquerading attack.

■ Password Guessing Attack

After the attacker extract the secret values (f_i, e_i) stored in the user's smart card under the described assumption, the attacker attempts to derive the user's password PW_i using $r_i=h(PW_i \oplus K) \oplus f_i$ in the registration phase. However, the attacker cannot guess the user's password PW_i using the secret values extracted from the legitimate user's smart card, because the attacker does not know the secret value r_i. Hence, the proposed scheme is secure against off-line password guessing attack.

■ Insider attack

In the registration phase, if the user's password PW_i and personal biometrics B_i are revealed to the server, the insider of the server may directly obtain PW_i, B_i and impersonate as the user to access user's other accounts in other server. But, the enhanced scheme is secure for the insider attack, because the user submits $h(K \oplus PW_i)$ instead of PW_i and $h(K \oplus B_i)$ in stead of B_i.

■ Mutual Authentication

As described in the above subsection, the enhanced scheme can withstand the user impersonation attack and the server masquerading attack, consequently the proposed scheme provides mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret values (f_i, e_i) stored in the user's smart card, the user can be authenticated to the server and the server can be authenticated to the user. Because the attacker cannot make the login request message {ID_i, M_2, M_3}, the reply message {M_6, M_7} without knowing the secret value X_s kept by the server.

V. Conclusions

In this paper, we analyzed the security weaknesses of Das's scheme. And we have shown that Das's scheme is still insecure against the user impersonation attack, the server masquerading attack, the off-line password guessing attack and the insider attack. Also, we proposed the enhanced scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, the enhanced scheme is secure against the user impersonation attack, the server masquerading attack, the off-line password guessing attack, and the insider attack. And we can see that the enhanced scheme provides mutual authentication between the user and

the server.

References

[1] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics 46, pp. 28-30, 2000

[2] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further Improvements of an Efficient Password based Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics 50(2), pp. 612-614, 2004

[3] M. L. Das, A. Sxena and V. P. Gulathi, "A Dynamic ID-based Remote User Authentication Scheme", IEEE Transactions on Consumer Electronics 50(2), pp. 629-631. 2004

[4] C. W. Lin, C. S. Tsai and M. S. Hwang, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions", Journal of Computer and Systems Sciences International, Vol. 45, No.4, pp. 623-626, 2006

[5] C. S. Bindu, P. C. S. Reddy and B. Satyanarayana, "Improved Remote User Authentication Scheme Preserving User Anonymity", International Journal of Computer Science and Network Security 8(3), pp. 62-66, 2008

[6] W. C. Ku, S. T. Chang and M. H. Chiang, "Further Cryptanalysis of Fingerprint-based Remote User Authentication Scheme Using Smart Cards", Electronics Letters, Vol. 41, No. 5, pp. 240-241 (2005)

[7] M. K. Khan, J. Zhang, "An Efficient and Practical Fingerprint-based Remote User Authentication Scheme with Smart Cards", ISPEC 2006, LNCS 3903, pp. 260-268, 2006

[8] C. C. Chang, S. C. Chang and Y. W. Lai, "An Improved Biometrics-based User Authentication Scheme without Concurrency System", International Journal of Intelligent Information Processing, Vol. 1, No. 1, pp. 41-49, 2010

[9] C. T. Li, M. S Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, Vol. 33, pp. 1-5, 2010

[10] A. K. Das, "Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards", IET Information Security Vol.5, Iss. 3, pp. 145-151, 2011

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

[12] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Transactions on Computers 51(5), pp. 541-552, 2002

저자 소개

안 영 화(정회원)

- 성균관대학교 전자공학과 박사
- 해군사관학교 전자공학과 교수
- 강남대학교 학술정보처장
- 강남대학교 전산정보원장
- 미국 Florida State University 방문교수
- 현 강남대학교 컴퓨터미디어공학부 교수

<주관심분야 : 시스템 보안, 네트워크 보안, 정보 보안>

주 영 도(정회원)

- 한양대학교 전자통신공학과 학사
- 미국 University of South Florida 컴퓨터공학과 석사
- 미국 Florida State University 전산학과 박사
- KT 통신망 연구소 선임연구원
- 시스코 시스템즈 코리아 상무
- 화웨이 기술 코리아 부사장
- 현 강남대학교 컴퓨터미디어공학부 교수

<주관심분야 : 정보보안, 네트워크 보안, 정보검색>