韓國컴퓨터情報學會 論文誌
第17卷 第2號, 2012. 2.

2012-17-2-4-3

Security Analysis and Improvements of a Biometrics-based User Authentication Scheme Using Smart Cards

Young-Hwa An*

스마트 카드를 이용한 생체인식 기반 사용자 인증 스킴의 안전성 분석 및 개선

안 영 화*

Abstract

Many biometrics-based user authentication schemes using smart cards have been proposed to improve the security weaknesses in user authentication system. In 2010, Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system which can withstand forgery attack, off-line password guessing attack, replay attack, etc. In this paper, we analyze the security weaknesses of Chang et al.'s scheme and we have shown that Chang et al.'s scheme is still insecure against man-in-the-middle attack, off-line biometrics guessing attack, and does not provide mutual authentication between the user and the server. And we proposed the improved scheme to overcome these security weaknesses, even if the secret information stored in the smart card is revealed. As a result, the proposed scheme is secure for the user authentication attack, the server masquerading attack, the man-in-the-middle attack, and the off-line biometrics guessing attack, does provide the mutual authentication between the user and the remote server. And, in terms of computational complexities, the proposed scheme is more effective than Chang et al.'s scheme.

▸ Keyword : Authentication, Biometrics, Man-in-the-Middle Attack, Mutual Authentication

---

• 제1저자 : 안영화
• 투고일 : 2011. 12. 21, 심사일 : 2012. 01. 06, 게재확정일 : 2012. 01. 28.
* 강남대학교 컴퓨터미디어정보공학부(Division of Computer and Media Information Engineering, Kangnam University)
※ 이 논문은 2010년도 강남대학교 교내연구비 지원에 의한 것임

요 약

스마트카드를 이용한 생체인식 기반 사용자 인증 스킴이 인증 시스템에서 안전성 취약점을 개선하기 위해 제안되고 있다. 2010년 Chang 등은 위조 공격, 오프라인 패스워드 추측 공격, 재생 공격 등에 안전한 개선된 생체인식 기반 사용자 인증 스킴을 제안하였다. 본 논문에서는 Chang 등의 스킴에 대한 안전성을 분석하고, Chang 등의 스킴이 중간자 공격, 오프라인 생체인식 추측 공격 등에 취약하고, 사용자와 서버 사이에 상호인증을 제공하지 못함을 증명하였다. 그리고 본 논문에서는 이와 같은 안전성 취약점들을 개선한 인증 스킴을 제안하였다. 안전성 분석 결과, 제안된 스킴은 사용자 가장 공격, 서버 가장 공격, 중간자 공격, 오프라인 생체인식 추측 공격 등에 안전하고, 사용자와 서버 사이에 상호인증을 제공하고 있음을 알 수 있다. 그리고 계산 복잡도 관점에서 제안된 스킴은 Chang 등의 스킴보다 효율적임을 알 수 있다.

▸ Keyword : 인증, 생체인식, 중간자 공격, 상호인증

I. Introduction

With the increasing of users using commercial services through networks, the user authentication scheme using smart card has been becoming one of important security issues. However, security weaknesses have been exposed in the user authentication scheme due to the careless password management and the sophisticated attack techniques. Several schemes[1-6] have been proposed to improve security, efficiency, and cost.

Recently, personal biometrics information, such as fingerprints, faces, irises, hand geometry, and palm-prints, etc. has been used to design biometrics-based user authentication schemes[7-10]. There are several advantages of using biometrics key 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.

As described the above, biometrics-based remote user authentication schemes are inherently more reliable and secure than traditional password-based remote user authentication schemes.

In 2004, Jin et al.[7] proposed two-factor auth entication scheme using fingerprint data and tokenized pseudo random number. Using this new scheme proposed by Jin et al., in 2010, Li and Hwang[9 proposed an efficient biometrics-based remote user authentication scheme using smart cards. However, in 2010, Chang et al.[10] pointed out that Li and Hwang's scheme allowed an attacker to perform off-line guessing attack. And Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system that is secure against forgery attack, off-line guessing attack, and replay attack.

In this paper, if an attacker can access a user's smart card and extract the values stored in the smart card by monitoring the power consumption[11-12], we show that Chang et al.'s scheme is not secure against man-in-the middle attack, off-line biometrics guessing attack, and does not provide mutual authentication between the user and the server. And we propose the improved scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed.

This paper is organized as follows. In section II, we briefly review Chang et al.'s scheme. In section III, we describe the security weaknesses of Chang et al.'s scheme. The proposed scheme is presented in section IV, and its security analysis and performance evaluations are given in section V. Finally, the

conclusions are given in section VI.

II. Review of Chang et al.'s Scheme

In this section, we briefly review Chang et al.'s scheme[10]. The security of this scheme is based on hash function and random nonce to withstand the forgery attack, the off-line guessing attack and the replay attack. Chang et al.'s scheme is divided into three phases: registration phase, login phase, and authentication phase. We present the illustration of registration phase in Fig. 1. and login and authentication phase in Fig. 2. And the notations used in this paper are listed below:

- U: The user
- S: The server
- R: The registration centre
- ID: Identity of user
- X_s: Secret information kept by the server
- Q: Biometric information of the user
- N_u: A nonce chosen by user
- N_s: A nonce chosen by server
- h(): One-way hash function
- ‖: Concatenation
- ⊕: Exclusive-OR operation
- A≟B: Whether A equals B or not

2.1 Registration Phase

This phase works whenever the user registers to the registration centre and obtains the smart card.

1) The user submits his identifier ID and the personal biometrics Q to the registration centre through a secure channel.
2) Upon receiving the information, the registration centre selects a random number R_1, and then computes $f=Q \oplus R_1$ and $m=h(ID \| X_s) \oplus f$, where R_1 is the first time random secret to protect the biometrics.
3) The registration centre issues the information {ID, h(), R_1, f, m} to the smart card and sends it to the user through a secure channel.

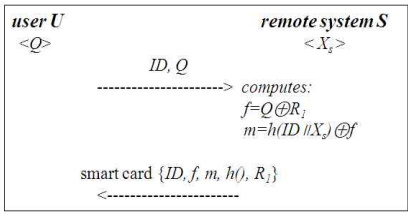

Fig. 1. Registration Phase in Chang et al.'s Scheme

2.2 Login Phase

This phase works whenever the user wants to login to the remote server.

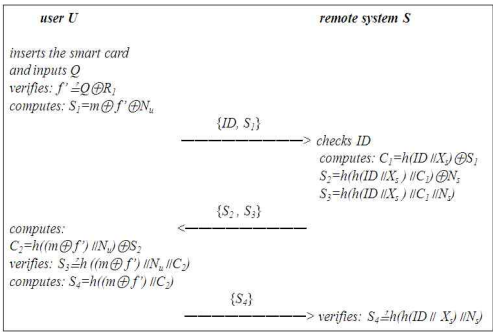

Fig. 2. Login Phase and Authentication Phase in Chang et al.'s Scheme

1) The user inserts his smart card into a card reader and provides the personal biometrics Q on the specific device.
2) The smart card computes $f'=Q \oplus R_1$, and verifies whether f'equals f or not.
3) If it holds, the smart card generates a random nonce N_u and computes $S_1=m \oplus f' \oplus N_u$.
4) And then, the user sends the message {ID, S_1} to the remote server.

2.3 Authentication Phase

This phase works whenever the remote server received the user's login request.

1) The server checks the format of ID. If it holds, the server computes $C_1=h(ID \| X_s) \oplus S_1$.
2) The server computes $S_2=h(h(ID \| X_s) \| C_1) \oplus N_s$ and $S_3=h((h(ID \| X_s) \| C_1) \| N_s)$, where N_s is a random nonce selected by server.

3) The server sends the message $\{S_2, S_3\}$ to the user.
4) Upon receiving the message, the smart card computes $C_2=h((m\oplus f')\|N_u)\oplus S_2$, and verifies whether S_3 equals $h((m\oplus f')\|N_u\|C_2)$ or not.
5) If it holds, the user authenticates the server as a legal server, and then computes $S_4=h((m\oplus f')\|C_2)$.
6) The user sends the message $\{S_4\}$ to the server.
7) Upon receiving the message, the server verifies whether S_4 equals $h(h(ID\|X_s)\|N_s)$ or not.
8) If it holds, the server authenticates the user as a legal user and accepts the user's login request.

After performing the above three phases, Chang et al.'s scheme provides the mutual authentication between the user and the server.

III. Security Weaknesses of Chang et al.'s Scheme

In this section, we analyze the security of Chang et al.'s scheme. To analyze the security weaknesses, we assume that an attacker can access a user's card and extract the values stored in the smart card by monitoring the power consumption[11-12] and intercept the messages communicating between the user and the server.

3.1 Man-in-the-Middle Attack

Under the above assumption, after an attacker extracts m, f from a user's smart card, he can easily derive $h(ID\|X_s)$ by computing $m\oplus f=h(ID\|X_s)$. Now the attacker with the computed value can perform the man-in-the-middle attack like the following steps. The processing of the man-in-the-middle attack is illustrated in Fig. 3.

1) The attacker intercepts the login message $\{ID, S_1\}$ of other user, where S_1 is $m\oplus f'\oplus N_u$ comp uted by the server in the login phase. Then he computes $S_{1a}=h(ID\|X_s)\oplus N_a$, where N_a is a random nonce generated by the attacker.
2) The attacker sends the forged message $\{ID, S_{1a}\}$ to the server.
3) Upon receiving the forged message, the server checks the validity of ID. If it holds, the server accepts the login request message generated by the attacker.
4) The server computes the following equations, and then the server sends the reply message $\{S_2, S_3\}$ to the user .

$$C_1= h(ID\|X_s)\oplus S_{1a}$$
$$S_2=h(h(ID\|X_s)\|C_1)\oplus N_s$$
$$S_3=h(h(ID\|X_s)\|C_1\|N_s)$$

where N_s is a random nonce generated by the server.
5) The attacker intercepts the reply message $\{S_2, S_3\}$, and then computes $S_{2a}=h(h(ID\|X_s)\|N_u')\oplus N_a$ and $S_{3a}=h(h(ID\|X_s)\|N_u'\|N_a)$, where N_u' is the value N_u by computing $S_1\oplus h(ID\|X_s)$.
6) Then the attacker sends the forged reply message $\{S_{2a}, S_{3a}\}$ to the user.
7) Upon receiving the forged reply message, the smart card computes $C_2=h((m\oplus f')\|N_u)\oplus S_{2a}$, and then verifies whether S_{3a} equals $h((m\oplus f')\|N_u\|C_2)$ or not. If it holds, the user accepts the forged message generated by the attacker. Thus the attacker is authenticated by the user.
8) The smart card computes $S_4=h((m\oplus f')\|C_2)$, and then the user sends the message $\{S_4\}$ to the server for mutual authentication.
9) The attacker intercepts the message $\{S_4\}$ of the user, and then computes $S_{4a}=h(h(ID\|X_s)\|N_s')$, where N_s' is the value N_s by computing $S_2\oplus h(h(ID\|X_s)\|N_a)$.
10) The attacker sends the forged message $\{S_{4a}\}$ to the server.
11) Upon receiving the forged message, the server verifies whether S_{4a} equals $h(h(ID\|X_s)\oplus N_s)$ or not. If it holds, the server accepts the forged message generated by the attacker. Thus the attacker is authenticated by the server.

As described the above, the attacker can masquerade as the legal user while talking to the server and masquerade as the legitimate server while talking to the user.

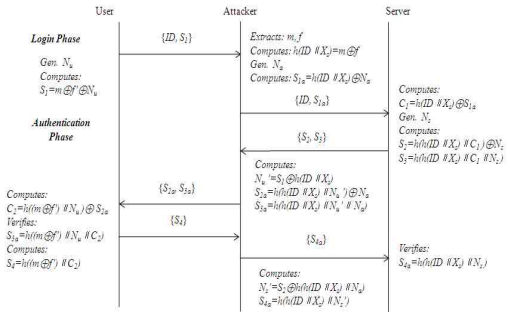

Fig. 3. Man-in-the-Middle Attack

3.2 Biometrics Guessing Attack

As described the above, we assume that the attacker can extract the secret values (f, R_1) from the legal user's smart card by some means. Now, the attacker can easily find out the biometrics information of the user by computing the Q=f $\oplus R_1$. In Chang et al.'s scheme, this biometrics information is very important secret value because it is necessary to confirm personal identity in registration and login phase. If an attacker gets this secret biometrics information, the attacker can use it to impersonate a legal user who wants to register with this system.

3.3 Mutual Authentication

As described the above, such as the man-in-the-middle attack, Chang et al.'s scheme fails to provide the mutual authentication between the user and the remote server. That is, if the attacker can extract the secret values (f, m) from the legal user's smart card and intercepts the messages communicating between the user and the server, the attacker can impersonate the legal user easily by computing the equation $S_{1a}=h(ID \| X_s) \oplus N_a$. Also, if the attacker can extract the secret values (f, m) from the legal user's smart and intercepts the messages, the attacker can masquerade the legal remote server easily by computing the equation $S_{2a}=h(h(ID \| X_s) \| N_u^*) \oplus N_a$ and $S_{3a}=h(h(ID \| X_s) \| N_u^* \| N_a)$.

IV. The Proposed Scheme

In this section, we propose an improved Chang et al.'s scheme which can withstand the man-in-the-middle attack, the biometrics guessing attack and the insider attack. The proposed scheme is divided into three phases: registration phase, login phase and authentication phase. The registration phase is illustrated in Fig. 4. Also, the login and authentication phase is illustrated in Fig. 5.

4.1 Registration Phase

This phase works whenever the user registers to the registration centre and obtains the smart card.

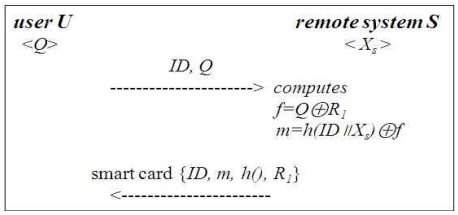

Fig. 4. Registration Phase in the Proposed Scheme

1) The user submits his identifier ID and the personal biometrics Q to the registration centre through a secure channel.
2) Upon receiving the information, the registration centre generates random number R_1, and then computes f=Q $\oplus R_1$ and m=h(ID $\|$ X_s)$\oplus$f, where R_1 is the first time random secret to protect the biometrics.
3) The registration centre issues the information {ID, m, h(), R_1} to the smart card and sends it to the user through a secure channel.

4.2 Login Phase

This phase works whenever the user wants to login to the remote server.

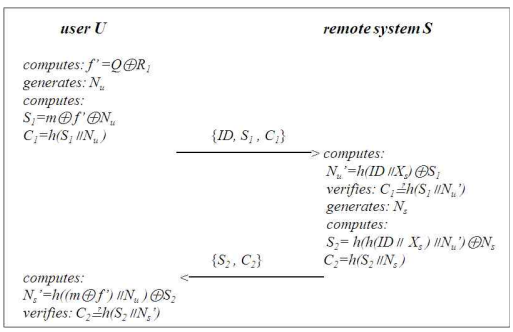

Fig. 5. Login Phase and Authentication Phase in the Proposed Scheme

1) The user inserts his smart card into a card reader and provides the personal biometrics Q on the specific device.
2) The smart card computes $f'=Q\oplus R_1$, and verifies whether f' equals f or not.
3) If it holds, the smart card generates a random nonce N_u and computes:

$$S_1=m\oplus f'\oplus N_u$$
$$C_1=h(S_1 \| N_u)$$

4) And then, the user sends the message {ID, S_1, C_1} to the remote server.

4.3 Authentication Phase

This phase works whenever the remote server received the user's login request.

1) The server computes $N_u'=h(ID \| X_s)\oplus S_1$, and then verifies whether C_1 equals $h(S_1 \| N_u')$ or not.
2) If it holds, the server accepts the login message from the user and authenticates the user as a legal user.
3) And then the server generates N_s and computes the following equations.

$$S_2=h(h(ID \| X_s) \| N_u')\oplus N_s$$
$$C_2=h(S_2 \| N_s)$$

4) The server sends the message {S_2, C_2} to the user.
5) Upon receiving the message, the smart card computes $N_s'=h((m\oplus f') \| N_u)\oplus S_2$, and verifies whether C_2 equals $h(S_2 \| N_s')$ or not.
6) If it holds, the user accepts the reply message from the server and authenticates the server as a legal server.

After performing the above three phases, the proposed scheme provides the mutual authentication between the user and the server.

V. Security Analysis and Performance Evaluations of the Proposed Scheme

In this section, we will provide the security analysis of the proposed scheme based on one-way hash function and personal biometrics. Also we will evaluate the performance of the proposed scheme in terms of computation.

5.1 Security Analysis

To analyze the security of the proposed scheme, we assume that can access a user's smart card and extract the values stored in the smart card by some means[11-12], and intercepts the messages communicating between the user and the server. Here, we only discuss the user impersonation attack, the server masquerading attack, the man-in-the-middle attack, the biometrics guessing attack, and the mutual authentication.

5.1.1 User Impersonation Attack

To impersonate as the legal user, an attacker attempts to make the forged login request massage which can be authenticated to the server. However, the attacker cannot impersonate as the user by forging the login request massage, because the attacker does not compute the forged message S_1^* or C_1^* without knowing the remote server's secret value X_s and the user's personal biometrics Q. Hence, the attacker has no chance to login by launching the user impersonation attack.

5.1.2 Server Masquerading Attack

To masquerade as the legal 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 does not compute S_2^* or C_2^* without knowing the remote server's secret value X_s and the user's personal biometrics Q. Hence, the attacker has no chance to be masqueraded as the legal server to the user by launching the server masquerading attack.

5.1.3 Man-in-the-Middle Attack

To perform the man-in-the-middle attack, an attacker attempts to make the forged massages {ID, S_{1a}}, {S_{2a}, S_{3a}} and {S_{4a}} each phase. However, the attacker cannot perform the forged massages, because the attacker does not compute these forged messages without knowing the remote server's secret value X_s and the user's personal biometrics Q, even if

the attacker has known the secret information in the user's smart card. Hence, the attacker cannot impersonate as the legal user while communicating to the server, and cannot masquerade as the legitimate server while communicating to the user.

5.1.4 Biometrics guessing attack

To perform the biometrics guessing attack, the attacker attempts to extract the secret values from the user's smart card under the described assumption. Then the attacker attempts to derive the user's personal biometrics Q by computing $Q=f\oplus R_1$ in the registration phase. However, the attacker cannot guess the user's personal biometrics Q, because the attacker does not know the secret value f computed by the server. Hence, the proposed scheme withstand against the off-line biometrics guessing attack.

5.1.5 Mutual Authentication

As described the above subsection, such as the user impersonation attack and the server masquerading attack, the proposed scheme provide the mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret information 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 attempt to make the forged messages each phase without knowing the remote server's secret value X_s and the user's personal biometrics Q.

Table 1. Security comparison of the proposed scheme to Chang et al.'s scheme

security components	Chang et al.'s scheme	the proposed scheme
User Impersonation Attack	possible	impossible
Server Masquerading Attack	possible	impossible
man-in-the-middle attack	possible	impossible
biometrics guessing attack	possible	impossible
mutual authentication	impossible	possible

From the above studies, the security comparison of the proposed scheme to Chang et al.'s scheme is summarized in Table 1. We can see that the proposed scheme is relatively more secure than Chang et al.'s scheme.

5.2 Performance Evaluations

In this section, we evaluate the efficiency of the proposed scheme in terms of the computational complexities by comparing with Chang et al.'s scheme. In Table 2, we can see that the proposed is relatively more effective in terms of computational complexities than Chang et al.'s scheme, even if the proposed scheme does provide the security against the various attacks.

Table 2. Computational complexities comparison of the proposed scheme to Chang et al.'s scheme

phase	Chang et al.'s scheme	the proposed scheme
registration phase	1TH+2TX	1TH+2TX
login phase	3TX	1TH+3TX
authentication phase	7TH+3TX	6TH+3TX

*TH: the time for performing a one-way hash function, TX: the time for performing a exclusive-OR operation

VI. Conclusions

In this paper, we analyzed the security weaknesses of Chang et al.'s scheme. And we have shown that Chang et al.'s scheme is still insecure against man-in-the-middle attack, off-line biometrics guessing attack, and does not provide mutual authentication between the user and the server. And we proposed the improved scheme to overcome these security weaknesses, while preserving all merits of Chang et al.'s scheme, even if the secret information stored in the smart card is revealed. As a result of security analysis, the proposed scheme is secure for the user authentication attack, the server masquerading attack, the man-in-the-middle attack, and the off-line biometrics guessing attack. In addition, we

can see that the proposed scheme provide the mutual authentication between the user and the remote server. And, in terms of computational complexities, the proposed scheme is more effective than Chang et al.'s scheme.

References

[1]. J.J. Shen, C.W. Lin and M.S. Hwang, "Security Enhancement for the Timestamp-based Password Authentication Scheme Using Smart Cards," Computers and Security, 22(7), pp.591-595, 2003.

[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, Vol.50, No.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, Vol.50, No.2, pp.629-631, 2004.

[4]. 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, Vol.8, No.3, pp.62-66, 2008.

[5]. Y. Lee, D. Won, "Cryptanalysis and Enhancement of a Remote User Authentication Scheme Using Smart Cards," Journal of The Korea Society of Computer and Information, Vol. 15, N0. 1, pp. 139-147, 2010.

[6]. S.M. Seo, Y.H. An, "Security Improvements on the Remote User Authentication Scheme Using Smart Cards," Journal of The Korea Society of Computer and Information, Vol. 15, No. 3, pp. 91-97, 2010.

[7]. A.T.B. Jin, D.N.C. Ling and A. Goh, "Biohashing: two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number," Pattern Recognition, Vol.37, pp.2245-2255, 2004.

[8]. M.K. Khan, J. Zhang, "Improving the Security of a Flexible Biometrics Remote User Authentication Scheme," Computer Standards and Interfaces, Vol.29, No.1, pp.82-85, 2007.

[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]. 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.

[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, Vol.51, No.5, pp.541-552, 2002.

저 자 소 개

안 영 화

1975 : 성균관대학교 전자공학과 공학사

1977 : 성균관대학교 전자공학과 공학석사

1990 : 성균관대학교 전자공학과 공학박사

현 재 : 강남대학교 컴퓨터미디어정보공학부 교수

관심분야 : 정보보안, 네트워크 보안

Email : yhan@kangnam.ac.kr