

Security Weaknesses of an Improved Biometrics-based User Authentication Scheme without Concurrency System

Young-Hwa An*

*Computer Media Information Engineering, Kangnam University,
111, Gugal-dong, Giheung-gu, Yongin-si, Gyeonggi-do, 446-702, Korea
yhan@kangnam.ac.kr

Abstract— Recently, 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 the forgery attack, the off-line password guessing attack, the replay attack, etc. In this paper, we analyze the security weaknesses of Chang et al.'s scheme, and we will show that Chang et al.'s scheme is still vulnerable to the user impersonation attack, the server masquerading attack and the biometric guessing attack, and does not provide the mutual authentication between the user and the remote server.

Keywords— Authentication, Biometrics, User Impersonation Attack, Server Masquerading Attack, Mutual Authentication

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]-[7] 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[8]-[13]. 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 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.[8] proposed two-factor authentication

scheme using fingerprint data and tokenized pseudo random number. Using this new scheme proposed by Jin et al., in 2010, Li and Hwang[11] proposed an efficient biometrics-based remote user authentication scheme using smart cards. However, in 2010, Chang et al.[12] pointed out that Li and Hwang's scheme allowed an attacker to perform the off-line password guessing attack. And Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system that is secure against the forgery attack, the off-line password guessing attack, and the 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 or analyzing the leaked information[14]-[16], we show that Chang et al.'s scheme is not secure against the user impersonation attack, the server masquerading attack, and the biometrics guessing attack. And we can show that Chang et al.'s scheme also does not provide the mutual authentication between the user and the remote server.

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. Finally, conclusions are made in section IV.

II. REVIEW OF CHANG ET AL.'S SCHEME

In this section, we briefly review Chang et al.'s scheme[12]. The security of this scheme is based on hash function and random nonce to withstand the forgery attack, the off-line password 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
- $\parallel$: Concatenation
- $\oplus$: Exclusive-OR operation

A. Registration Phase

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

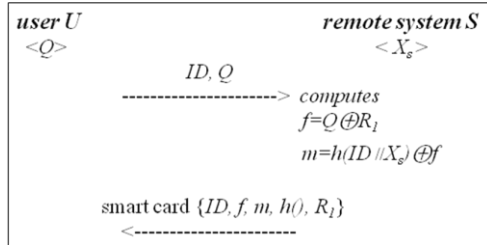


Figure 1. Registration Phase in Chang et al.'s Scheme

- 1) The user submits his identifier ID and the personal biometrics Q to the registration centre through a secure channel.
- 2) Upon receiving the submitted information, the registration centre selects a random number R_1 , and then computes:

$$f = Q \oplus R_1$$

$$m = h(ID \parallel X_s) \oplus f$$

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.

B. Login Phase

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

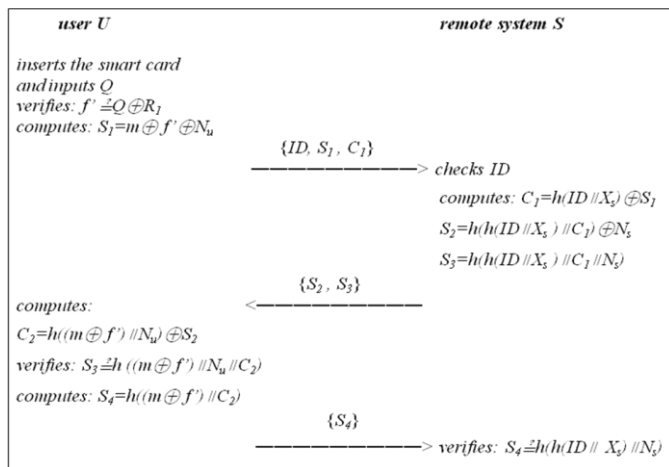


Figure 2. Login Phase and Authentication Phase in Chang et al.'s Scheme

- 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 user 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.

C. Authentication Phase

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

- 1) The server checks the format of ID.
- 2) If it holds, the server computes $C_1 = h(ID \parallel X_s) \oplus S_1$ using $h(ID \parallel X_s)$.
- 3) The server computes:

$$S_2 = h(h(ID \parallel X_s) \parallel C_1) \oplus N_s$$

$$S_3 = h(h(ID \parallel X_s) \parallel C_1 \parallel N_s)$$

where N_s is a random nonce selected by the server.

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

After performing the above 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 could obtain the secret values stored in the smart card illegally by monitoring the power consumption or analyzing the leaked information[14]-[16] and intercept the messages communicating between the user and the server.

A. User Impersonation Attack

As described the above, we assume that the attacker can extract the secret values (f, m) from the user's smart card illegally by some means and intercepts the message $\{S_1\}$ communicating between the user and the server. The procedure of the user impersonation attack is like the

following steps. Also, the user impersonation attack is illustrated in Fig.3.

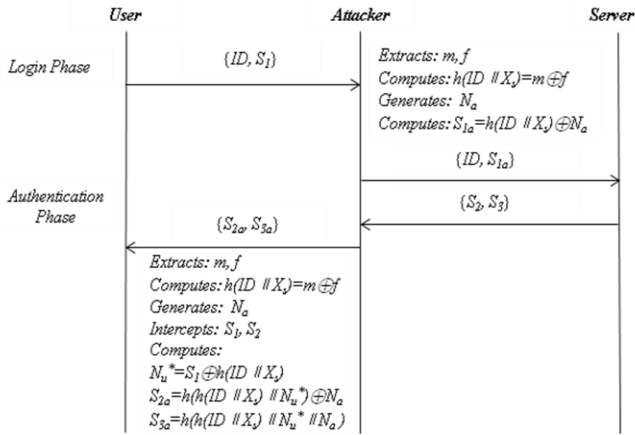


Figure 3. User Impersonation Attack and Server Masquerading Attack

1) In the registration phase, the attacker computes easily $h(ID \parallel X_s) = f \oplus m$ using the extracted secret values (f, m) from the legal user's smart card.

2) And then, the attacker generates random nonce N_a , and then computes $S_{1a} = h(ID \parallel X_s) \oplus N_a$.

3) The attacker sends the forged message {ID, S_{1a} } to the remote server.

4) Upon receiving the message, the remote server checks the format of ID. If it holds, the remote server will be convinced that the message is sent from the user. And then the remote server will compute $N_a^* = h(ID \parallel X_s) \oplus S_{1a}$ and make the return message S_2, S_3 .

Therefore, the attacker without knowing the biometrics information of the user can impersonate as the legal user.

B. Server Masquerading Attack

As described the above, we assume that the attacker can extract the secret values (f, m) from the user's smart card illegally by some means and intercepts the message $\{S_1\}$ communicating between the user and the server. The procedure of the server masquerading attack is like the following steps. Also, the server masquerading attack is illustrated in Fig.2.

1) In the registration phase, the attacker computes easily $h(ID \parallel X_s) = f \oplus m$ using the extracted secret values (f, m) from the legal user's smart card.

2) And then, the attacker computes $N_u^* = h(ID \parallel X_s) \oplus S_1$, and then generates random nonce N_a .

3) The attacker computes:

$$S_{2a} = h(h(ID \parallel X_s) \parallel N_u^*) \oplus N_a$$

$$S_{3a} = h(h(ID \parallel X_s) \parallel N_u^* \parallel N_a)$$

4) The attacker sends the forged message $\{S_{2a}, S_{3a}\}$ to the user.

5) Upon receiving the message, the smart card computes $N_a^* = h((m \oplus f) \parallel N_u) \oplus S_{2a}$, and then checks whether S_{3a} equals the value of $h((m \oplus f) \parallel N_u \parallel N_a^*)$ using the computed N_a^* or not.

6) If it holds, the user will be convinced that the message is sent from the remote server. And then the user will compute the return message $S_4 = h((m \oplus f) \parallel N_a^*)$.

Therefore, the attacker without knowing the biometrics information of the user can masquerade as the remote server.

C. Biometrics Guessing Attack

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

D. Mutual Authentication

As described in above subsection, such as the user impersonation attack and the server masquerading 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, the attacker can impersonate the legal user easily by computing the equation $S_{1a} = h(ID \parallel X_s) \oplus N_a$. Also, if the attacker can extract the secret values (f, m) from the legal user's smart and intercepts the message $\{S_1\}$ communicating between the user and the server, the attacker can masquerade the legal remote server easily by computing the equation $S_{2a} = h(h(ID \parallel X_s) \parallel N_u^*) \oplus N_a$ and $S_{3a} = h(h(ID \parallel X_s) \parallel N_u^* \parallel N_a)$.

IV. CONCLUSIONS

In 2010, Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system which can withstand the forgery attack, the off-line password guessing attack, the 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 vulnerable to the user impersonation attack, the server masquerading attack and the biometrics guessing attack. In addition, we can see that Chang et al.'s scheme fails to provide the mutual authentication between the user and the remote server.

ACKNOWLEDGMENT

This work was supported by Kangnam University Research Grant in 2011.

REFERENCES

- [1] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

- [2] M.S.Hwang and L.H.Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, pp. 28-30, 2000.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] J. Xu, W.T. Zhu and D.G. Feng, "Improvement of a Fingerprint-based Remote User Authentication Scheme," *International Journal of Security and its Applications(IJNSA)*, Vol. 2, No. 3, 2008.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] A.K. Das, "Cryptanalysis and Further Improvement of a Biometric-Based Remote User Authentication Scheme Using Smart Cards," *International Journal of Security and its Applications(IJNSA)*, Vol. 3, No. 2, 2011.
- [14] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," *Proceedings of Advances in Cryptology*, pp. 388-397, 1999.
- [15] 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.
- [16] E. Brier, C. Clavier and F. Oliver, "Correlation Power Analysis with a Leakage Model," *Lecture Notes in Computer Science*, Vol. 3156, pp. 135-152, 2004.