Security Weaknesses of a Biometric-Based Remote User Authentication Scheme Using Smart Cards

Younghwa An

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

Abstract

To improve the security weaknesses in user authentication system, many biometrics-based user authentication schemes using smart cards have been proposed. Das in 2011, proposed an effective biometric-based remote user authentication scheme using smart cards that can provide strong authentication and mutual authentication, while eliminating the security flaws of Li-Hwang's scheme. In this paper, we analyze the security 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, the man-in-the-middle attack and the insider attack. In addition, Das's scheme does not provide mutual authentication between the user and the server.

Keywords: *Biometrics, User Authentication Attack, Server Masquerading Attack, Mutual Authentication*

1. 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 researches [1-15] have been proposed to improve security, reliability, and efficiency in the user authentication scheme.

In traditional identity-based remote user 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 and lost. Therefore, several biometrics-based remote user authentication schemes [10-15] 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 [14] 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 [15], in 2011, pointed out that Li-Hwang's scheme does not resolve security flaws in login and authentication, security drawbacks in password change phase and security 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, 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 the various attacks. In addition, we show that Das's scheme does not provide mutual authentication between the user and the server. To analyze the security of Das's scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [16, 17] and intercept messages communicating between the user and the server. And, we assume that an attacker may possess the capabilities to thwart the security schemes.

- An attacker has total control over the communication channel between the user and the server in the login and authentication phase. That is, the attacker may intercept, insert, delete, or modify any message across the communication procedures.
- An attacker may (i) either steal a user's smart card and then extract the secret values stored in the smart card, (ii) or steal a user's password, but cannot commit both of (i) and (ii) at a time.

If both of the user's smart card and password was stolen at the same time, then there is no way to prevent an attacker from impersonating as the user. Therefore, a remote user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

This paper is organized as follows. In Section 2, we briefly review Das's scheme. In Section 3, we describe the security weaknesses of Das's scheme. Finally, the conclusions are presented in Section 4.

2. Reviews of Das's scheme

In 2011, Das 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. We use the notations shown in Table 1.

Table 1. Notations Used in this Paper

Notation	Description
C_i	User i
R_i	Trusted registration centre i
S_i	Server i
A_i	Attacker i
PW_i	Password of the user i
ID_i	Identity of the user i
B_i	Biometric template of the user i
h()	A secure hash function
X_s	A secret information maintained by the server
$x \| y$	x concatenates with y
$x \oplus y$	Exclusive-OR operation of x and y

2.1. Registration Phase

Before logging in the remote server S_i, a user C_i initially has to register to the trusted registration centre R_i as the following steps. The registration phase is illustrated in Figure 1.

R1. C_i submits his identity ID_i and password PW_i to R_i through a secure channel. Also the user inputs his biometrics information B_i on the specific device to R_i.

R2. 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.

R3. 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.

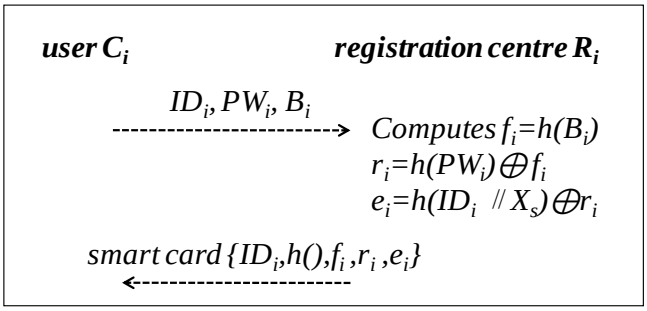


Figure 1. Registration Phase of the Das's Scheme

2.2. Login Phase

When the user C_i wants to login the remote server S_i, the user has to perform the following steps. The login and authentication phase are illustrated in Figure 2.

L1. C_i inserts his smart card into a card reader and inputs the personal biometrics information B_i on the specific device to verify the user's biometrics. If the biometrics information matches the template stored in the system, C_i passes the biometrics verification.

L2. 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' equals r_i, the smart card computes the following equations, where R_c is a random number generated by the smart card.

$$M_1=e_i\oplus r_i'$$
$$M_2=M_1\oplus R_c$$
$$M_3=h(R_c)$$

L3. C_i sends the message $\{ID_i, M_2, M_3\}$ to S_i.

2.3. Authentication Phase

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

A1. S_i checks the format of ID_i.

A2. If the ID_i is valid, S_i computes $M_4=h(ID_i \| X_s)$, $M_5=M_2\oplus M_4$.

A3. S_i verifies whether $M_3=h(M_5)$ or not. If they are equal, S_i computes the following equations, where R_s is a random number generated by the server.

$$M_6=M_4 \oplus R_s$$
$$M_7=h(M_2 \| M_5)$$
$$M_8= h(R_s)$$

A4. Then, S_i sends the message $\{M_6, M_7, M_8\}$ to C_i.

A5. After receiving the message, C_i verifies whether $M_7=h(M_2 \| R_c)$ or not. If they are equal, C_i computes $M_9=M_6 \oplus M_1$.

A6. C_i verifies whether $M_8=h(M_9)$ or not. If they are equal, C_i computes $M_{10}=h(M_6 \| M_9)$

A7. Then, C_i sends the message $\{M_{10}\}$ to S_i.

A8. 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.

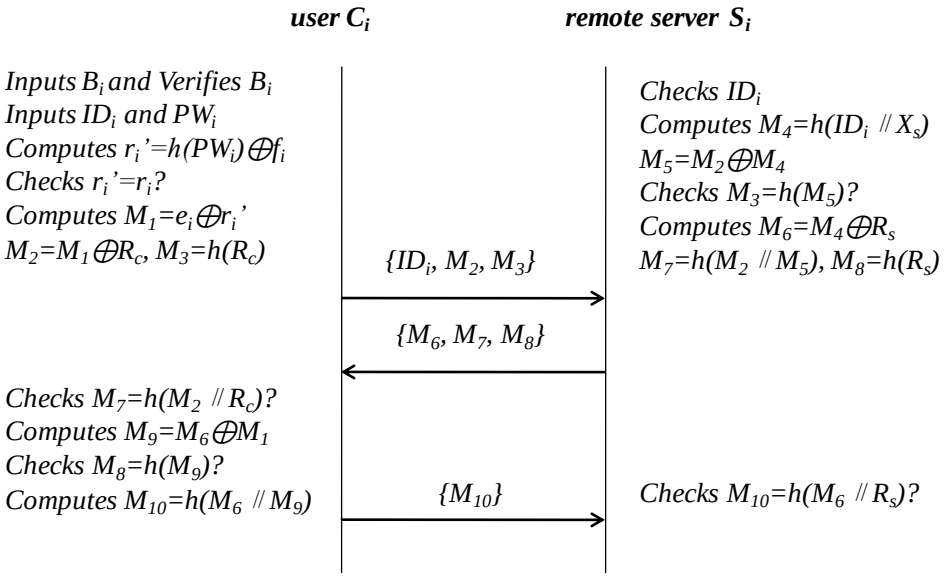


Figure 2. Login and Authentication Phase of the Das's Scheme

3. Security Weaknesses of Das's Scheme

In this section, we will analyze the security weaknesses in Das's biometric-based remote user authentication scheme. To analyze the security weaknesses, we assume that an attacker could extract the secret values stored in the smart card by monitoring the power consumption [16, 17] and intercept messages communicating between the user and the server. Under this assumption, we will discuss the various attacks such as the user impersonation attack, the server masquerading attack, the password guessing attack, the man-in-the-middle attack, the insider attack, and the mutual authentication between the user and the server.

3.1. User Impersonation Attack

If the attacker can obtain 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 attacker can perform the user impersonation attack as the following steps. The procedure of the user impersonation attack is illustrated in figure 3.

UA1. The attacker A_i computes the following equations, where R_{ac} is a random number chosen by the attacker.

$$M_{a1}=e_i \oplus r_i$$
$$M_{a2}=M_{a1} \oplus R_{ac}$$
$$M_{a3}=h(R_{ac})$$

UA2. Then, A_i sends the forged message {ID_i, M_{a2}, M_{a3}} to the remote server S_i.

UA3. Upon receiving the forged message, S_i checks the format of ID_i. If it holds, S_i computes $M_4=h(ID_i \| X_s)$, $M_5=M_{a2} \oplus M_4$.

UA4. S_i 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 legal user.

UA5. 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.

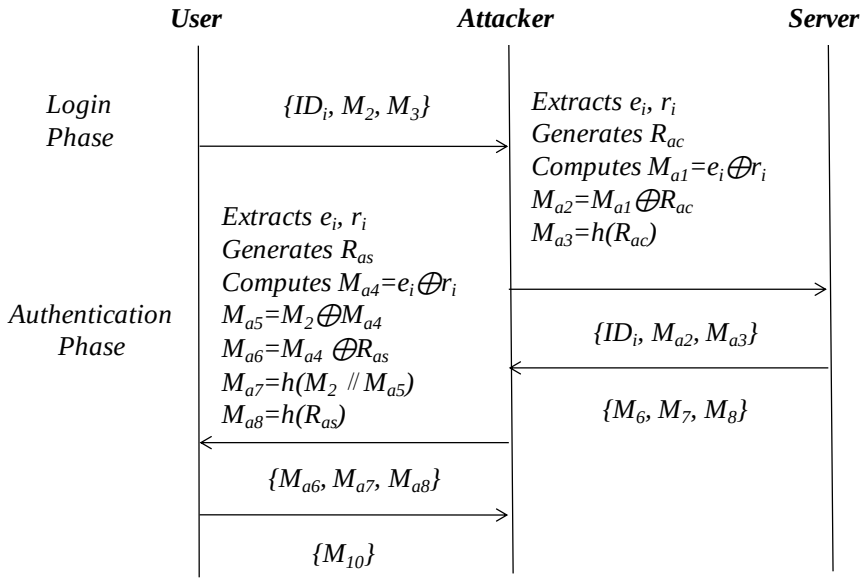


Figure 3. User Impersonation Attack and Server Masquerading Attack

3.2. Server Masquerading Attack

If the attacker can obtain 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 attacker can perform the server masquerading attack as the following steps. The procedure of the server masquerading attack is illustrated in Figure 3.

SA1. The attacker A_i computes the following equations, where R_{as} is a random number chosen by the attacker.

$$M_{a4}=e_i \oplus r_i$$
$$M_{a5}=M_2 \oplus M_{a4}$$
$$M_{a6}=M_{a4} \oplus R_{as}$$
$$M_{a7}=h(M_2 \| M_{a5})$$
$$M_{a8}=h(R_{as})$$

SA2. Then, A_i sends the forged message $\{M_{a6}, M_{a7}, M_{a8}\}$ to the user C_i.

SA3. 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 $M_9=M_{a6} \oplus M_1$.

SA4. C_i 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 legal server.

SA5. Then, C_i makes the reply massage $\{M_{10}\}$ by computing $M_{10}= h(M_{a6} \| M_9)$ in the authentication phase.

3.3. Password Guessing Attack

If an attacker can extract the secret values (r_i, f_i) from the legal user's smart card by some means, the attacker can easily find out PW_i by performing the password guessing attack, in which each guess PW_i^* for PW_i can be verified by the following steps.

PA1. The attacker A_i computes the secret parameter $r_i^*=h(PW_i^*) \oplus f_i$ from the registration phase.

PA2. A_i verifies the correctness of PW_i^* by checking $r_i=r_i^*$.

PA3. A_i 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.

3.4. Man-in-the-Middle Attack

To perform the man-in-the-middle attack, an attacker attempts to make the forged massages in the login phase and in the authentication phase. Unfortunately, in Das's scheme, the attacker can perform the man-in-the-middle attack, because the attacker can compute the forged login massage $\{ID_i, M_{a2}, M_{a3}\}$ in the login phase and the forged reply massage $\{M_{a6}, M_{a7}, M_{a8}\}$ in the authentication phase if the attacker can obtain the secret values (e_i, r_i) stored in the user's smart card by some means and intercept the legitimate massages communicating between the server and the user.

3.5. Insider Attack

In the registration phase, if the user's password PW_i and biometrics information B_i are revealed to the server, the insider of the server may directly obtain the user's password and biometrics information. Thus the insider of the server 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.

3.6. Mutual Authentication

Generally, if 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. Therefore, Das's scheme fails to provide mutual authentication as described the above subsection 3.1, 3.2. Namely, if the attacker can obtain the secret values (e_i, r_i) from the legal user's smart card by some means and intercept the messages communicating between the user and the server, the attacker can make the forged messages 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 forged messages easily by computing $M_{a6}=M_{a4} \oplus R_{as}$, $M_{a7}=h(M_2 \| M_{a5})$, $M_{a8}=h(R_{as})$ in the authentication phase.

4. Conclusions

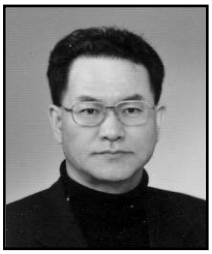
Recently, Das proposed an effective biometric-based remote user authentication scheme using smart cards and has maintained that his scheme can provide strong authentication with eliminating the security flaws of Li-Hwang's scheme. In this paper, we discuss the security flaws of Das's scheme and have shown that Das's scheme is still vulnerable to the user impersonation attack, the server masquerading attack, the off-line password guessing attack, the man-in-the-middle attack and the insider attack. In addition, we can see that Das's scheme fails to provide mutual authentication between the user and the server.

References

[1] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] M. S. Hwang and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, **(2000)**, pp. 28-30.
[3] 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, **(2004)**, pp. 612-614.
[4] 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, **(2004)**, pp. 629-631.
[5] 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, **(2006)**, pp. 623-626.
[6] 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, **(2008)**, pp. 62-66.
[7] J. Y. Liu, A. M. Zhou and M. X. Gao, "A New Mutual Authentication Scheme based on Nonce and Smart Cards", Computer Communications, vol. 31, **(2008)**, pp. 2205-2209.
[8] H. C. Hsiang and W. K. Shih, "Improvement of the Secure Dynamic ID based Remote User Authentication Scheme for Multi-Server Environment", Computer Standards and Interfaces, vol. 31, **(2009)**, pp. 1118-1123.
[9] C. C. Lee, T. H. Lin and R. X. Chang, "A Secure Dynamic ID based Remote User Authentication Scheme for Multi-Server Environment using the Smart Cards", Expert System with Applications, vol. 38, **(2011)**, pp. 13863-13870.

[10] C. H. Lin and Y. Y. Lai, "A Flexible Biometric Remote User Authentication Scheme", Computer Standards and Interfaces, vol. 27, no. 1, **(2004)**, pp. 19-23.
[11] 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, **(2005)**, pp. 240-241.
[12] M. K. Khan and J. Zhang, "An Efficient and Practical Fingerprint-based Remote User Authentication Scheme with Smart Cards", ISPEC 2006, LNCS 3903, **(2006)**, pp. 260-268.
[13] 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, **(2010)**, pp. 41-49.
[14] C. T. Li and M. S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, vol. 33, **(2010)**, pp. 1-5.
[15] A. K. Das, "Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards", IET Information Security, vol. 5, Issue 3, **(2011)**, pp. 541-552.
[16] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", Proceedings of Advances in Cryptology, **(1999)**, pp. 388-397.
[17] 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, **(2002)**, pp. 541-552.

Author



Younghwa An received his B.S. and M.S. degrees in electronic engineering from Sungkyunkwan University, Korea in 1975 and 1977, respectively. He obtained his Ph. D. in information security from same university, 1990. From 1983 to 1990, he served as an assistant professor with the department of electronic engineering at Republic of Korea Naval Academy. Since 1991, he has been a professor with department of computer and media information engineering at Kangnam University. During his tenure at Kangnam University, he served as the director of computer & information center and the director of central library. He performed research as a visiting professor at Florida State University from 2002 to 2003. His major research interests include information security and network security.