International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.129-136
http://dx.doi.org/10.14257/ijsia.2015.9.12.13

Enhanced Biometric-based User Authentication Protocol Using Non-tamper Resistant Smart Cards

Minsu Park[1] and Hyunsung Kim[2]

[1]*Dept. of Cyber Security, Kyungil University*
Kyungsan, Kyungbuk 712-701, Korea
parkminsu34@naver.com
[2](*Corresponding Author*) *Dept. of Cyber Security, Kyungil University*
Kyungsan, Kyungbuk 712-701, Korea
kim@kiu.ac.kr

Abstract

This paper reviews An's enhanced biometric-based user authentication protocol and shows that it is weak against the password guessing attack and has a problem of verification in the authentication phase. They are very important features to be secured to the user authentication protocol. Furthermore, this paper proposes an enhanced biometric-based user authentication protocol using non-tamper resistant smart cards to solve the problems in An's protocol. The overall security analyses show that the proposed protocol could achieve the desired security goals.

Keywords: *Security, Authentication, Biometric-based, Password, Non-temper resistant, Smart card.*

1. Introduction

One of the fundamental problems in the areas of cryptography and communication security is authentication to enable two parties communicating over a public network to establish a high-entropy secret key from their low entropy passwords [1]. Many password based authentication protocols were designed to solve this problem and often showed the security vulnerabilities including password guessing attack, replay attack, insider attack, and many more attacks [2-8].

To solve the problems in the password based authentication, several biometrics-based authentication schemes have been designed [9-13]. There are some advantages of using biometrics as compared to the traditional passwords, which are 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, and someone's biometrics is not easy to break than others [13].

Kim *et al.* proposed an ID-based remote user authentication scheme based on biometrics [9]. They claimed that their scheme is secure against various attacks. However, Scott showed that Kim *et al.*'s scheme is weak against some attacks [14]. Quite recently, Das proposed an efficient biometrics-based remote user authentication scheme using smart cards and argued that his protocol is secure against the user impersonation attack, the server masquerading attack, the parallel session attack and the stolen password attack, and the scheme provides mutual authentication [12]. However, An showed that Das's scheme is weak against user impersonation attack, server masquerading attack, password guessing attack, and insider attack, and does not provide

ISSN: 1738-9976 IJSIA

mutual authentication. Furthermore, he provides a remedy scheme on Das's scheme [13].

This paper shows that An's protocol has weakness of the password guessing attack and has a lack of verification in the authentication phase. Furthermore, this paper proposes an enhanced biometric-based user authentication protocol with non-tamper resistant smart card, which could solve the overall problems in An's protocol. The overall security analyses show that the proposed protocol achieves the desired security goals.

2. Review of An's Protocol

This section provides a review of An's enhanced biometric-based user authentication protocol [13]. The protocol is divided into three phases: registration phase, login phase and authentication phase. Table 1 shows the notations used in this paper.

Table 1. Notations

Symbol	Description
U_i	The i^{th} user
S_i	The remote server
R_i	The trusted registration center
ID_i	The identity of user U_i
PW_i	The password of user U_i
B_i	The biometric information of user U_i
R_c, R_s, K, R_a, a, b	The random numbers
SK	The session key between U_i and S
$h(\cdot)$	The collision free one-way hash function
$\oplus$	The bitwise XOR operation
$\|\|$	The string concatenation operation

2.1. Registration Phase

Before logging to the remote server S_i, a user U_i initially has to register to the trusted registration center R_i as the following steps.

(R1) U_i submits his (or her) identity ID_i and password information $h(PW_i \oplus K)$ to R_i through a secure channel. Also U_i submits his (or her) biometrics information $h(B_i \oplus K)$ via the specific device to R_i, where K is a random number generated by U_i.

(R2) 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 key generated by the server.

(R3) R_i stores (ID_i, $h()$, f_i, e_i) on U_i's smart card and sends it to U_i via a secure channel. And U_i stores the random number K into the smart card issued by R_i.

2.2. Login Phase

When U_i wants to login S_i, U_i has to perform the following steps.

(L1) U_i inserts his (or her) smart card into a card reader and inputs the biometrics information B_i on the specific device to verify user's biometrics. If the biometrics information $h(B_i \oplus K)$ matches f_i stored in the smart card, U_i passes the verification.

(L2) U_i inputs ID_i and PW_i, and then the smart card computes the following equations, where R_c is a random number generated by the smart card :

$r_i' = h(PW_i \oplus K) \oplus f_i$,

$M_1 = e_i \oplus r_i'$,

$M_2 = M_1 \oplus R_c$,

$M_3 = h(M_1 || R_c)$.

(L3) U_i sends the login request message $\{ID_i, M_2, M_3\}$ to S_i.

2.3. Authentication Phase

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

(A1) S_i checks the format of ID_i.
(A2) If ID_i is valid, S_i computes $M_4 = h(ID_i || X_s)$ and $M_5 = M_2 \oplus M_4$.
(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 S_i:
$M_6 = M_4 \oplus Rs$,
$M_7 = h(M_2 || M_5)$,
$M_8 = h(R_s)$.
(A4) Then, S_i sends the message $\{M_6, M_7, M_8\}$ to U_i.
(A5) After receiving the message, U_i verifies whether $M_7 ? = h(M_2 || R_c)$ or not. If they are equal, U_i computes $M_9 = M_6 \oplus M_1$.
(A6) U_i verifies whether $M_8 ? = h(M_9)$ or not. If they are equal, U_i computes $M_{10} = h(M_6 || M_9)$.
(A7) Then, U_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 U_i's login request.

3. Security Analysis of An's Protocol

This section shows that An's protocol is weak against password guessing attack. Furthermore, An's protocol has a problem of verification in the authentication phase. To provide the security analyses of An's protocol, we assumed that attacker could steal and read the smart card, and could control the insecure channel completely since the messages from the legal user are sent to the server through an insecure channel [15-16].

3.1. Password Guessing Attack with Lost Smart Card

This sub-section shows that An's protocol is vulnerable to the password guessing attack with smart cards. Knowing the password is very important in An's protocol to form a legalized login message. Password guessing attack with lost smart card considers an additional assumption to the password guessing attack that attacker has more power to get user's smart card.

With the assumption, first of all, an attacker steals the user's smart card and reads the memory on it. The attacker chooses a new password candidate PW_i' from dictionary. Using the known values ID_i, $h()$, f_i, e_i and K from the smart card and M_2 and M_3 from the intercepted messages $\{ID_i, M_2, M_3\}$, $\{M_6, M_7, M_8\}$ and $\{M_{10}\}$, the attacker computes $M_1' = e_i \oplus h(PW_i' \oplus K) \oplus f_i$ and $R_C' = M_1' \oplus M_2$. Finally the attacker verifies if $h(M_1' || R_C')$ is equal to M_3 on the intercepted message. If they are equal, the attacker could make sure that his/her guess is right. Otherwise, the attacker repeats the whole guessing process

again and again until the correct one come out. Thereby, An's protocol is weak against password guessing attack.

3.2. Problem of Verification

An's protocol does not provide a proper authentication to the registered user due to the A3 step in the authentication phase. S_i validates legal user by verifying the equivalence between the computed $h(M_5)$ and the received M_3. However, the validation always does not hole because $h(M_5)=h(M_2 \oplus M_4)=h(e_i \oplus r_i' \oplus R_c \oplus h(ID_i||X_s))=h(R_c)$ and $M_3=h(M_1||R_c)=h(e_i \oplus r_i'||R_c)=h(h(ID_i||X_s)||R_c)$. It means that S_i need to check the equivalent of $h(R_c)$ and $h(h(ID_i||X_s)||R_c)$ to check the authenticity of the user, which does not hold in any cases due to the parameters difference. Thereby, $h(M_5)$ needs to be changed with $h(M_4||M_5)=h(h(ID_i||X_s)||R_c)$ for the proper verification of legal users.

4. Enhanced Biometric-Based User Authentication Protocol

This section proposes an enhanced biometric-based user authentication protocol with non-tamper resistant smart cards to solve the weaknesses in An's protocol. The proposed protocol is divided into three phases: registration phase, login phase and authentication phase.

4.1. Registration Phase

When a user U_i wants to subscribe services from S_i, U_i needs to perform the following steps.

(R1) U_i selects a random number R_A, inputs U_i's identity ID_i, password PW_i and biometrics B_i, computes $DPW_i=h(PW_i||R_A)$ and $f_i=h(B_i||R_A)$ and submits { ID_i, DPW_i, f_i } to the registration server R_i through a secure channel.

(R2) R_i computes $r_i=DPW_i \oplus f_i$ and $e_i=h(ID_i||x) \oplus r_i$, where x is a secret key generated and kept by R_i. R_i issues a smart card by storing { $h()$, f_i, e_i } to U_i.

(R3) After receiving the smart card, U_i computes $DR_A=R_A \oplus ID_i \oplus PW_i$ and stores it into the smart card.

4.2. Login Phase

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

(L1) U_i inserts his (or her) smart card into a card reader and inputs ID_i', PW_i' and B_i', and computes $R_A'=DR_A \oplus ID_i' \oplus PW_i'$ and $h(B_i'||R_A')$. If $h(B_i||R_A')$ matches with f_i stored in the smart card, U_i is authenticated by the smart card.

(L2) Only if the smart card verifies U_i successfully, it generates a random number a and computes $r_i'=h(PW_i'||R_A') \oplus f_i$, $Y'=e_i \oplus r_i'$, $M_1=Y' \oplus a$, and $MAC_1=h(Y'||ID_i||h(a))$.

(L3) U_i sends the login request { ID_i, M_1, MAC_1 } to S_i.

4.3. Authentication Phase

After receiving the login request, S_i has to perform the following steps.

(A1) S_i computes $Y^*=h(ID_i||x)$ and $a^*=M_1 \oplus Y^*$. After that, S_i checks the validity of MAC_1 by comparing it with S_i's computation of $h(Y^*||ID_i||h(a^*))$. If the verification is successful, S_i chooses a random number b and computes $SK=h(Y^*||h(a^*)||h(b))$,

$M_2=Y^* \oplus b$ and $MAC_2=h(SK||h(a^*)||h(b))$ and sends the reply message { M_2, MAC_2 } to U_i.

(A2) After receiving the message, U_i computes $b'=M_2 \oplus Y'$ and $SK'=h(Y||h(a)||h(b'))$ and checks the validity of MAC_2 by comparing it with U_i's computation of $h(SK'||h(a)||h(b'))$. If the verification is successful, U_i authenticates S_i and believes that the session key is agreed with S_i safely.

5. Security Analysis

This section provides security analysis for the proposed protocol with the concern of non-tamper resistant smart cards. The proposed protocol is secure against various attacks and provides mutual authentication.

5.1. User Impersonation Attack

To impersonate as the legitimate user, an attacker attempts to make a forged login request which could pass the authentication check by the server. However the attacker cannot impersonate as the legitimate user by forging the login request message in the proposed protocol even if the attacker can extract the secret information { $h()$, f_i, e_i, DR_A } stored in the user's smart card. It is mainly because the attacker cannot compute a correct new login request message { ID_i, M_1, MAC_1 } without computing the proper MAC_1 due to the lack of knowledge on $Y=h(ID_i||x)$, which is secured based on the one-way hash function. Hence, the attacker has no chance to form a proper login request to be authenticated by the server in the proposed protocol and thereby it is secure against the user impersonation attack.

5.2. Server Masquerading Attack

To masquerade as the legitimate server, an attacker attempts to make a forged reply message, which can be masqueraded as a legal server to the user. However the attacker cannot masquerade as the server by forging the reply message, because the attacker cannot compute the proper MAC_2, which needs to compute SK, due to the lack of knowledge on $h(a)$ and $Y=h(ID_i||x)$. Hence, the attacker cannot masquerade as the legitimate server to the user by launching the server masquerading attack.

5.3. Password Guessing Attack

After the attacker extracts the secret information { $h()$, f_i, e_i, DR_A } stored in the user's smart card under the assumption, the attacker attempts to derive a proper password PW_i of the user. To perform the attack, the attacker needs to know R_A first from DR_A. However, it is infeasible to the attacker due to the lack of knowledge on ID_i and PW_i. Even if the attacker could know ID_i from the previous intercepted message, the attacker could not know any information related with PW_i due to the one way hash function. Thereby, the proposed protocol could cope from the password guessing attack even with the assumption of the usage of non-tamper resistant smart card.

5.4. Insider Attack

In the registration phase, if the user's password PW_i and the biometrics information B_i are revealed to the server, the insider of the server may directly obtain them and impersonate as the user to access user's other accounts in other servers. However, the proposed protocol is secure against this attack because the user uses the amplified

information $h(PW_i||R_A)$ and $h(B_i||R_A)$ instead of the real information PW_i and B_i, respectively.

5.5. Mutual Authentication

As described in the previous sub-sections of user impersonation attack and server masquerading attack, the proposed protocol can withstand the user impersonation attack and the server masquerading attack, consequently the proposed protocol provides mutual authentication between the user and the server. Namely, even if the attacker can extract the secret information { $h()$, f_i, e_i, DR_A } stored in the user's smart card, only the legal user can be authenticated to the server but not the attacker. Since the attacker cannot make any legal login request { ID_i, M_1, MAC_1 } and any legal reply message { M_2, MAC_2 } without knowing PW_i, $h(ID_i||x)$ and the parameters to compute MAC_1 and MAC_2. Thereby, the proposed protocol provides mutual authentication between the user and the server.

6. Conclusion

This paper had shown that An's protocol has weak against the password guessing attack and has a verification problem in the authentication phase. For the password guessing attack, it is assumed that attacker could steal a legal user's smart card and read the memory on it. Furthermore, we proposed a remedy protocol to solve the problems in An's protocol, which uses non-tamper resistant smart cards as the reasonable assumption with smart cards. The security analysis shows that the proposed protocol has good aspects in the security aspects.

Acknowledgments

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] J. Nam, K. K. R. Choo, M. Park, J. Paik, D. Won, "On the Security of a Simple Three-Party Key Exchange Protocol without Server's Public Keys," The Scientific World Journal, vol. 2014, article ID 479534, **(2014)**.
[2] S. W. Lee, H. Kim, K. Y. Yoo, "Efficient Password-based Authenticated Key Agreement Protocol," Lecture Notes in Computer Science, vol. 3046, **(2004)**, pp. 617-626.
[3] H. Kim, "Remote User Authentication Scheme with Key Agreement Providing Forward Secrecy," Journal of Security Engineering, vol. 12, no. 1, **(2015)**, pp. 1-12.
[4] S. W. Lee, H. Kim, K. Y. Yoo, "Improved efficient remote user authentication scheme using smartcards," IEEE Trans. on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 565-567.
[5] S. W. Lee, H. Kim, K. Y. Yoo, "Improvement of HWWM-authenticated key agreement protocol," Applied Mathematics and Computation, vol. 162, no. 3, **(2005)**, pp. 1315- 1320.
[6] S. W. Lee, H. Kim, K. Y. Yoo, "Improvement of Lee and Lee's authenticated key agreement scheme," Applied Mathematics and Computation, vol. 162, no. 3, **(2005)**, pp. 1049- 1053.
[7] S. W. Lee, H. Kim, K. Y. Yoo, "Efficient nonce-based remote user authentication scheme using smart cards," Applied Mathematics and Computation, vol. 167, **(2005)**, pp. 355-361.
[8] H. Kim, "Location-based Authentication Protocol for First Cognitive Radio Networking Standard," Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 1160- 1167.
[9] H. Kim, S. W. Lee, K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, **(2003)**, pp. 32- 41.
[10] W. C. Ku, S. T. Chang, M. H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," Electronics Letters, vol. 41, no. 5, **(2005)**, pp. 240-241.

[11] C. C. Chang, S. C. Chang, 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.
[12] A. K. Das, "Analysis and Improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 4, **(2011)**, pp. 541-552.
[13] Y. An, "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards," Journal of Biomedicine and Biotechnology, vol. 2012, Article ID 519723, **(2012)**.
[14] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," ACM Operating Systems Review, vol. 38, no. 2, **(2004)**, pp. 73-75.
[15] S. Cho, S. W. Lee, H. Kim, "Improved Biometrics-based Remote User Authentication Scheme," Journal of Security Engineering, vol. 8, no. 1, **(2011)**, pp. 1-11.
[16] I. S. Jeon, H. Kim, "Enhanced Password-based Remote User Authentication Scheme using Smart Cards," Journal of the Korea Industrial Information System Society, vol. 16, no. 1, **(2011)**, pp. 9-19

Authors

Minsu Park, He is a student at the Department of Cyber Security, Kyungil University, Korea from 2012. He has been attended Information Security Laboratory supervised by Prof. Hyunsung Kim from 2012 and as a researcher at Research Institute of Information Cross-over Security at Kyungil University, respectively. His research interests include smartphone security, smart greed security, cloud computing security, digital forensics, information security, network security and ubiquitous computing security.

Hyunsung Kim, He is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.