Security Enhancements of a Remote User Authentication Scheme Preserving User Anonymity

Younghwa An and Hyungkyu Yang

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

Abstract

Recently, user authentication scheme in e-commerce and m-commerce has been becoming one of important security issues. In 2008, Bindu et al. proposed an improved remote user authentication scheme preserving user anonymity. In this paper, we analyze the security of Bindu et al.'s authentication scheme, and we demonstrate that their scheme is still insecure against the man-in-the-middle attack, the password guessing attack, and does not provide the user anonymity. Also, we propose an enhanced scheme to withstand the security weaknesses of Bindu et al.'s scheme, even if the secret information stored in the smart card is revealed. As a result of security analysis, we prove that the enhanced scheme is secure for the various attacks known by literatures, and provides the user anonymity, the session key agreement, and the mutual authentication between the user and the server.

Keywords: *Authentication scheme, User anonymity, Session key agreement, Man-in-the-middle attack*

1. Introduction

With the increasing number of e-commerce and m-commerce applications, the user authentication scheme using smart cards have been becoming one of important security issues. Several improved schemes [1-7] for remote user authentication schemes using smart card have been proposed.

In 2004, Das, *et al.*, [8] proposed a dynamic ID-based remote user authentication scheme using smart cards which allows users to change their password freely and provides user anonymity. In 2005, Chien, *et al.*, [9] pointed out that Das, *et al.*'s scheme does not provide user anonymity, and proposed an improved remote user authentication scheme preserving user anonymity. However, in 2008, Bindu, *et al.*, [10] pointed out that Chien, *et al.*'s scheme allowed an attacker to perform the man-in-the-middle attack. And Bindu, *et al.*, proposed an improved remote user authentication scheme preserving user anonymity which is secure against the replay attack, the password guessing attack, and the man-in-the-middle attack.

In this paper, we analyze the security of Bindu, *et al.*'s scheme, and we show that Bindu et al.'s scheme is not secure against the man-in-the-middle attack, the password guessing attack, and does not provide the user anonymity. Also, we propose an enhanced scheme to remove these security flaws of Bindu, *et al.*'s authentication scheme while preserving their merits, even if the secret information stored in the smart card is revealed.

This paper is organized as follows. In Section 2, we briefly review Bindu, *et al.*'s scheme. In Section 3, we describe the security weaknesses of Bindu, *et al.*'s scheme. In Section 4, we propose the enhanced scheme, and describe the security analysis and performance evaluations of the enhanced scheme in Section 5. Finally, conclusions are made in Section 6.

2. Reviews of Bindu, *et al.*'s Scheme

In 2008, Bindu, *et al.*, [10] proposed an improved remote user authentication scheme preserving user anonymity. Bindu, *et al.*'s scheme consists of three phases: registration phase, login phase, and authentication phase. The notations used in this paper are listed in Table 1.

Table 1. Notations and Descriptions

Notation	Description
U_i	User i
ID_i	Identity of user i
S	Remote server i
PW_i	Password of user i
x	Secret key of remote server
h()	One way hash function
$x \oplus y$	Exclusive-OR operation of x and y
$E_k[m]$	Encryption of m using key k
$D_k[m]$	Decryption of m using key k
p, g	Parameters of DH key exchange protocol

2.1. Registration Phase

This phase works whenever a user U_i initially registers to the remote server S.

R1. U_i submits his identity ID_i and hashed password $h(PW_i)$ to S through a secure channel.

R2. S computes $m=h(ID_i \oplus x) \oplus h(x) \oplus h(PW_i)$ and $I=h(ID_i \oplus x) \oplus x$.

R3. S issues a smart card to the user through a secure channel, where a smart card contains {m, I, h(), p, g}.

2.2. Login Phase

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

L1. U_i inserts his smart card into a card reader, and inputs his identity ID_i and password PW_i.

L2. The smart card generates a random number $r_u=g^v \bmod p$.

L3. The smart card computes:

$$M=m \oplus h(PW_i)$$
$$C=M \oplus r_u$$
$$R=I \oplus r_u$$

L4. U_i sends the message $\{C, T, E_R[r_u, ID_i, T]\}$ to S, where T is a current timestamp and $E_R[r_u, ID_i, T]$ is a cipher text of encrypted with the secret key R.

2.3. Authentication Phase

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

A1. The server computes $R=C \oplus h(x) \oplus x$ with the server's secret key x, and then decrypts the message $E_R[r_u, ID_i, T]$.

A2. The server checks the validity of the time interval between T and T', where T' is a timestamp when the server receives message.

A3. The server computes $h(ID_i \oplus x) \oplus x \oplus r_u$ using the extracted information r_u from the step A1. If the computed value equals R, the user's login request is accepted.

A4. The server sends the reply message $\{T_1, E_R[r_s, r_u+1, T_1]\}$ to the user, where $r_s=g^w \bmod p$ and T_1 is a current timestamp. And then the server can generate session key $K_{us}=r_u^w=g^{vw} \bmod p$.

A5. Upon receiving the message, the smart card checks the validity of the time interval and whether the decrypted data contains (r_u+1). If contains, the server is authenticated to the user, and the user can generate session key $K_{us}=r_s^v=g^{vw} \bmod p$.

A6. For the session key establishment, the user sends the message $E_{Kus}[r_s+1]$ to the server.

A7. The server decrypts the received message and checks the decrypted data, (r_s+1). If corrects, the server can be assured of a session key established between the server and the user.

3. Security Weaknesses of Bindu, *et al.*'s Scheme

In this section, we analyze the security of Bindu, *et al.*'s scheme. To analyze the security weaknesses of their scheme, we assume that an attacker is one of legitimate users and can extract the secret values stored in his own smart card by monitoring the power consumption or analyzing the leaked information [11-13] and intercept the messages communicating between the user and the server.

3.1. Man-in-the-middle Attack

A legitimate user U_i extracts (m, I) from his smart card, and then he derive $h(x) \oplus x$ by computing $h(x) \oplus x=m \oplus I \oplus h(PW_i)$. So, an attacker as the legitimate user with smart card can perform the man-in-the middle attack easily as the following steps. The man-in-the middle attack is illustrated in Figure 1.

M1. The attacker intercepts the login request message $\{C, T, E_R[r_u, ID_j, T]\}$ of other legitimate user j.

M2. The attacker computes $R=C \oplus h(x) \oplus x$, and then decrypts $E_R[r_u, ID_j, T]$.

M3. After generating a random number $r_a=g^a \bmod p$, the attacker computes:

$$R^*=R \oplus r_u \oplus r_a$$
$$C^*=C \oplus r_u \oplus r_a$$

M4. The attacker sends the forged login request message $\{C^*, T^*, E_{R*}[r_a, ID_j, T^*]\}$ to the server, where T^* is a current timestamp.

M5. Upon receiving the message, the server computes $R^*=C^* \oplus h(x) \oplus x$ and decrypts $E_{R*}[r_a, ID_j, T^*]$. Then the server sends message $\{T_1, E_{R*}[r_s, r_a+1, T_1]\}$ to the user, where $r_s=g^w \bmod p$.

M6. The attacker intercepts the reply message and decrypts $E_{R*}[r_s, r_a+1, T_1]$, and then the attacker can generate a session key $K_{as}=r_s^a=g^{aw} \bmod p$ between the attacker and the server.

M7. Also, the attacker sends the forged reply message $\{T_1^*, E_R[r_a, r_u+1, T_1^*]\}$ to the user, where T_1^* is a current timestamp.

M8. Upon receiving the message, the user checks the validity of the time interval and whether the decrypted data (r_u+1) is correct or not. If correct, the attacker is authenticated to the user. Then the attacker can generate a session key $K_{ua}=r_u^a=g^{va} \bmod p$ between the attacker and the user.

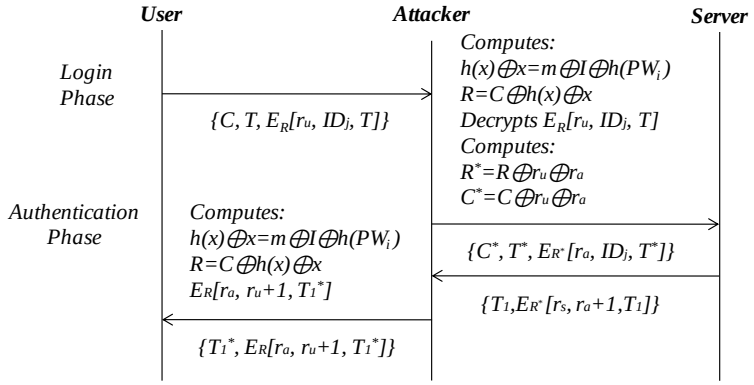

Figure 1. Man-in-the-middle Attack

3.2. Password Guessing Attack

Generally, most of users tend to select a password that is easily remembered for his convenience. Hence, these passwords are potentially vulnerable to the password guessing attack. To guess another legitimate user's password, we assume that an attacker as one of the legitimate users can extract the secret values (m, I) stored in his own smart card by monitoring the power consumption or analyzing the leaked information and intercept C from another user's login request message. Then the attacker can derive R by computing $R=C\oplus(m\oplus I\oplus h(PW_i))=C\oplus(h(x)\oplus x)$ with his own secret values.

Now, the attacker who has obtained another user's secret values (m, I, R, and C) can find out anther user' password PW_j by employing the password guessing attack, in which each guess PW_j^* for PW_j can be verified by the following steps.

P1. The attacker computes C^* in the login phase.

$$C^*=M^*\oplus r_u=(m\oplus h(PW_j^*))\oplus r_u$$
$$=(m\oplus h(PW_j^*))\oplus(R\oplus I)$$

P2. The attacker verifies the correctness of PW_j^* by checking $C^*=C$.

P3. The attacker repeats above steps until a correct password PW_j^* is found. Finally, the attacker can derive the correct password.

3.3. User Anonymity

To provide user anonymity, the scheme must not reveal the identity of user over insecure network. However, Bindu, *et al.*'s scheme does not provide user anonymity, because the attacker can easily obtain the identity of another legitimate user by computing R and decrypting $E_R[r_u, ID_j, T]\}$ in the login phase, if the attacker is one of the legitimate users.

4. The Enhanced Scheme

In this section, we propose an improved Bindu, *et al.*'s scheme which can not only withstand the password guessing attack, the user impersonation attack, the server masquerading attack, and the man-in-the-middle attack, but also provide the user anonymity, the session key agreement, and the mutual authentication between the user and the server. The enhanced scheme consists of three phases: registration phase, login phase and authentication phase. The login and authentication phase is illustrated in Figure 2.

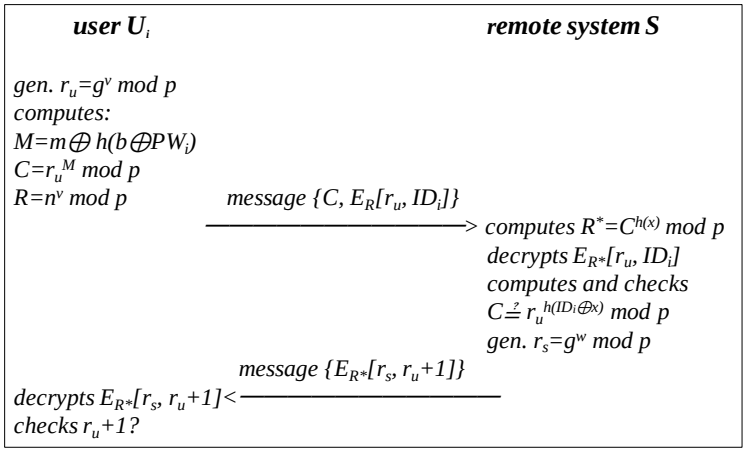

Figure 2. Login and Authentication Phase of the Enhanced Scheme

4.1. Registration Phase

This phase works whenever a user U_i initially registers to the remote server S.

R1. The user submits his identity ID_i and hashed password $h(b \oplus PW_i)$ to the server through a secure channel, where a random number b is generated by the user.

R2. The server computes $m=h(ID_i \oplus x) \oplus h(b \oplus PW_i)$ and $n=g^{h(IDi \oplus x)\ h(x)} \bmod p$, where x is a secret key of server.

R3. The server issues the smart card to the user through a secure channel, where a smart card contains {m, n, h(), p, g}.

R4. The user stores b into his new smart card so that the user does not need to remember b.

4.2. Login Phase

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

L1. The user inserts his smart card into a card reader, and inputs his identity ID_i and password PW_i.

L2. The smart card computes $M=m \oplus h(b \oplus PW_i)$.

L3. The smart card generates random number v, and computes:

$$r_u=g^v \bmod p$$
$$C=r_u^M \bmod p$$
$$R=n^v \bmod p$$

L4. The user sends a message $\{C, E_R[r_u, ID_i]\}$ to the server.

4.3. Authentication Phase

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

A1. The server computes $R^*=C^{h(x)} \bmod p$ using the server's secret key x, and then decrypts the message $E_R[r_u, ID_i]$.

A2. The server computes $r_u^{h(IDi \oplus x)} \bmod p$ using the extracted information r_u from the step A1. If the computed value equals C, the user is authenticated to the server.

A3. The server generates random number w, and computes $r_s=g^w \bmod p$. And then, the server generates session key, $K_{us}=r_u^w \bmod p=g^{vw} \bmod p$ between the user and the server.

A4. The server sends the reply message $\{E_{R*}[r_s, r_u+1]\}$ to the user.

A5. Upon receiving the message, the smart card decrypts the message $E_{R*}[r_s, r_u+1]$.

A6. The smart card checks the decrypted data, (r_u+1). If correct, the server is authenticated to the user.

A7. The user generates session key, $K_{us}=r_s^v=g^{vw} \bmod p$ between the user and the server.

A8. For the session key establishment, the user sends message $E_{Kus}[r_s+1]$ to the server.

A9. The server decrypts the received message, and checks the decrypted data, (r_s+1). If correct, the server can be assured of a session key established between the server and the user.

5. Security Analysis and Performance Evaluations of the Enhanced Scheme

In this section, we analyze the security of the enhanced scheme based on a one-way hash function, a discrete logarithm problem, and symmetric encryption/decryption.

5.1. Security Analysis

To analyze the security of the enhanced scheme, we assume that an attacker can obtain the values stored in the smart card by monitoring the power consumption or analyzing the leaked information [11-13] and intercept the messages communicating between the user and the server.

5.1.1. User Impersonation Attack: To impersonate a legitimate user, an attacker must make a forged login request massage to deceive the server. However, the attacker cannot impersonate the user by forging the login request massage $\{C, E_R[r_u, ID_i]\}$, because the attacker does not compute R or C without knowing the remote server's secret value x and the user's password PW_i. Hence, the attacker has no chance to login by launching the user impersonation attack.

5.1.2. Server Masquerading Attack: To masquerade as the server, an attacker must make a forged reply massage to deceive the user after receiving the user's login request message. However, the attacker cannot masquerade as the server by forging the reply massage $\{E_{R*}[r_s, r_u+1]\}$, because the attacker does not compute R or C without knowing the remote server's secret value x and the user's password PW_i. Hence, the attacker has no chance to be authenticated as the server to the user by launching the server masquerading attack.

5.1.3. Password Guessing Attack: According to the assumption, attacker can extract the secret values (m, n, b) from the legitimate user's smart card. Then the attacker attempts to derive the user's password PW_i using $m=h(ID_i \oplus x) \oplus h(b \oplus PW_i)$ or $n=g^{h(IDi \oplus x)\ h(x)}$ 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 remote server's secret value x. Hence, the enhanced scheme is secure for the password guessing attack.

5.1.4. Man-in-the-middle Attack: A registered user with a smart card cannot perform the man-in-the-middle attack because h(x) or x cannot be computed from the extracted secret values stored in his smart card and the intercepted messages communicating between the user and the server.

5.1.5. User Anonymity: To provide user anonymity, the enhanced scheme must not reveal the identity of user over an insecure network. In the enhanced scheme, even if an attacker is one of legitimate users, the attacker cannot compute R and $E_R[r_u, ID]$ using the secret values extracted from the legitimate user's smart card without knowing the encryption/decryption key in the login phase and authentication phase.

5.1.6. Mutual Authentication: As previously described in cases such as the user impersonation attack and the server masquerading attack, the enhanced scheme provides a mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret values 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 in each phase without knowing the remote server's secret value x.

5.1.7. Session Key Agreement: The session key $K_{us}=g^{vw} \bmod p$ is known to nobody except the user and the server, since the values $g^v \bmod p$, $g^w \bmod p$ are randomly chosen by the user and the server and encrypted them by the shared encryption key R.

The security analysis of Bindu, *et al.*'s scheme and the enhanced scheme is summarized in Table 2. The enhanced scheme is relatively more secure than Bindu, *et al.*'s scheme.

Table 2. Comparison the Proposed Scheme with Bindu, *et al.*'s Scheme

security feature	Bindu, *et al.*'s scheme[10]	the enhanced scheme
user authentication attack	possible	impossible
server masquerading attack	possible	impossible
password guessing attack	possible	impossible
man-in-the middle attack	possible	impossible
user anonymity	not provided	provide
mutual authentication	not provided	provide
session key agreement	not provided	provide

5.2. Performance Evaluations

In this section, we evaluate the efficiency of the enhanced scheme in terms of the computational complexities by comparing with Bindu, *et al.*'s scheme. In Table 3, the enhanced scheme requires five more modular exponential operations than Bindu, *et al.*'s scheme, because the enhanced scheme does provide the user anonymity, the mutual authentication and the session key agreement.

Table 3. Comparison the Enhanced Scheme with Bindu, *et al.*'s Scheme

phase	Bindu et al.'s scheme	the proposed scheme
registration phase	3TH+4TX	3TH+3TX+1TE+1TM
login phase	1TH+3TX+1TE+1TD	1TH+2TX+3TE+1TD
authentication phase	2TH+5TX+1TE+3TD	2TH+1TX+3TE+3TD

* TH: the time for performing a one-way hash function, TX: the time for performing a exclusive-OR operation, TE: the time for performing a modular exponential operation, TM: the time for performing a modular multiplication operation, TD: the time for performing a encryption/decryption operation

6. Conclusions

In this paper, we analyzed the security weaknesses of Bindu, *et al.*'s scheme and showed that Bindu, *et al.*'s scheme is still insecure against the man-in-the-middle attack, the password guessing attack, and that does not provide the user anonymity. Also, we proposed the enhanced scheme to withstand the security flaws of Bindu, *et al.*'s scheme, while preserving their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, we can see that the enhanced scheme is secure against the user authentication attack, the server masquerading attack, the password guessing attack and the man-in-the middle attack, as well as provide the user anonymity, the mutual authentication and the session key agreement.

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, vol. 22, no. 7, **(2003)**, pp. 591-595.
[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, **(2004)**, pp. 612-614.
[3] C. J. Fan, Y. C. Chan and Z. K. Zhang, "Robust Remote Authentication Scheme with Smart Cards", Computers and Security, vol. 24, no. 8, **(2005)**, pp. 619-628.
[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, **(2006)**, pp. 623-626.
[5] C. L. Lin and C. P. Hung, "Cryptanalysis and Improvement on Lee-Chen's One-Time Password Authentication Scheme", International Journal of Security and its Applications, vol. 2, no. 2, **(2008)**, pp. 1-8.
[6] J. Xu, W. T. Zhu and D. G. Feng, "Improvement of a Finger-Based User Authentication", International Journal of Security and its Applications, vol. 2, no. 3, **(2008)**, pp. 73-80.
[7] D. S. Wang and J. P. Li, "A Novel Mutual Authentication Scheme Based on Fingerprint Biometric and Nonce Using Smart Cards", International Journal of Security and its Applications, vol. 5, no. 4, **(2011)**, pp. 1-12.
[8] 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.

[9] H. Y. Chien and C. H. Chen, "A Remote Password Authentication Preserving User Anonymity", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA '05), **(2005)**.
[10] 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.
[11] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", Proceedings of Advances in Cryptology, **(1999)**, pp. 388-397.
[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, **(2002)**, pp. 541-552.
[13] E. Brier, C. Clavier and F. Oliver, "Correlation Power Analysis with a Leakage Model", Lecture Notes in Computer Science, vol. 3156, **(2004)**, pp. 135-152.

Authors

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.

Hyungkyu Yang received his B.S. and M.S. degrees in electronic engineering from Sungkyunkwan University, Korea in 1983 and 1985, respectively. He obtained his Ph. D. in Network security from same university, 1994. From 1985 to 1990, he served as the director of department of computer in Samsung Electronics. Since 1995, 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. His major research interests include information security and network security.