

Security Improvements of Dynamic ID-based Remote User Authentication Scheme with Session Key Agreement

Young-Hwa An*

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

Abstract—Password-based authentication schemes have been widely adopted to protect resources from unauthorized access. In 2010, Khan et al. proposed an efficient and secure dynamic ID-based authentication scheme to overcome the weaknesses of Wang et al.'s scheme. In this paper, we show that Khan et al.'s scheme is vulnerable to password guessing attack, forgery attack, and does not provide user anonymity. Also, we propose the improved scheme to overcome the security drawbacks of Khan et al.'s scheme and to provide user anonymity and session key agreement, even if the secret values stored in the smart card is revealed. As a result, the improved scheme is relatively more secure than the related scheme in terms of security.

Keywords—Authentication, Forgery Attack, Password Guessing Attack, Session Key Agreement, User Anonymity

I. INTRODUCTION

Password-based authentication scheme is one of the convenient and efficient authentication mechanics. However, numerous vulnerabilities have been disclosed in the authentication scheme due to careless password management and sophisticated attack techniques. Several improved schemes [1-11] for remote user authentication schemes have been proposed.

A common feature among most of the user authentication schemes is that the user's identity is static, which may leak some information about the user and create risk of ID-theft during the message transmission over an insecure channel. In 2004, Das et al. [4] proposed a dynamic ID-based remote user authentication scheme to overcome the risk of ID-theft or user impersonation. And Das et al. claimed that their scheme is secure against replay attack, forgery attack, insider attack, etc. However, later on, some researchers [5-7] pointed out that Das et al.'s scheme has some security drawbacks known in the literatures.

In 2009, Wang et al. [9] also pointed out that Das et al.'s scheme is susceptible to server spoofing attack and does not provide mutual authentication. Then, Wang et al. proposed a more efficient and secure dynamic ID-based remote user authentication scheme. However, Khan et al. in 2010 [11]

pointed out that Wang et al.'s scheme has insider attack and does not provide user anonymity and session key agreement. Then, they proposed an enhanced dynamic ID-based remote user authentication scheme, and claimed that their scheme can withstand the various known attacks and provide user anonymity and session key agreement

In this paper, we analyze the security weaknesses of Khan et al.'s scheme and we show that Khan et al.'s scheme is vulnerable to password guessing attack, forgery attack, and does not provide user anonymity. Also, we propose the improved scheme to overcome the security drawbacks of Khan et al.'s scheme, even if the secret values stored in the smart card is revealed. To analyze Khan et al.'s scheme, we assume that an attacker can extract the secret values stored in the smart card by monitoring the power consumption [12-13]. Also, 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.

Rest of the paper is organized as follows. In Section II, we briefly review Khan et al.'s scheme. In Section III, we describe the security weaknesses of Khan et al.'s scheme. The improved scheme is presented in Section IV, and its security analysis is given in Section V. Finally, conclusions are presented in Section VI.

II. REVIEW OF KHAN ET AL.'S SCHEME

In 2010, Khan et al. [11] proposed an efficient and secure dynamic ID-based authentication scheme. This scheme is divided into three phases: registration phase, login phase and

*This work was supported by Kangnam University Research Grant.

authentication phase. The notations used throughout this paper are in TABLE I.

TABLE I
NOTATION AND DEFINITION

Notation	Description
U_i	User i
S	Server
pw_i	Password of the user i
ID_i	Identity of the user i
$h()$	A secure hash function
x, y	A secret key kept by the server
$A \parallel B$	Concatenates A with B
$A \oplus B$	XOR operates A with B

A. Registration Phase

This phase is invoked whenever a user U_i initially wants to register to the remote server S .

- R1. U_i submits his identity ID_i and password information $RPW=h(r \parallel pw_i)$ to the server over a secure channel.
- R2. S computes $J=h(x \parallel IDU)$ and $L=J \oplus RPW$, where $IDU=(ID_i \parallel N)$ and N is a number of re-registering in the system.
- R3. S issues the smart card to U_i which contains values $\{L, y, h()\}$ over a secure channel.
- R4. U_i securely stores random number r in his smart card so that the user does not need to remember its value.

B. Login Phase

This phase works whenever the user U_i wants to login to the remote server S . The smart card performs the following steps.

- L1. The user inserts his smart card into a card reader, and inputs his ID_i and pw_i .
- L2. The smart card computes $RPW=h(r \parallel pw_i)$, $J=L \oplus RPW$ and $C_1=h(T_i \parallel J)$, where T_i is the current timestamp.
- L3. The smart card generates a random number d and computes an anonymous identity AID_i of U_i by computing $AID_i=ID_i \oplus h(y \parallel T_i \parallel d)$.
- L3. The user sends a login request message $\{AID_i, T_i, d, C_1\}$ to the server.

C. Authentication Phase

This phase works whenever the remote server S received the login request message. S verifies its authenticity by the following steps.

- A1. S verifies the validity of the time interval between T' and T_i , where T' is the current time when the login request message was received.
- A2. S computes $ID_i=AID_i \oplus h(y \parallel T_i \parallel d)$, and verifies the validity of the user's ID_i .
- A3. S checks the value of N in the database and computes $IDU=(ID_i \parallel N)$.
- A4. S computes $J=h(x \parallel IDU)$ and checks whether $h(T_i \parallel J)=C_1$ or not. If they are equal, the user's login request is accepted and the user is authenticated by the remote server.

A5. For mutual authentication, S computes $C_2=h(C_1 \oplus J \oplus T_s)$, where T_s is a current timestamp. Then, S sends the mutual authentication message $\{C_2, T_s\}$ to U_i .

A6. Upon receiving the message, U_i verifies the validity of the time interval between T'' and T_s , where T'' is the current time when mutual authentication message was received.

A7. U_i checks whether $h(C_1 \oplus J \oplus T_s)=C_2$ or not. If they are equal, the server is authenticated to the user.

A8. Now, U_i and S share the session key $S_k=h(C_2 \oplus J)$ for performing further operations.

III. SECURITY WEAKNESSES OF KHAN ET AL.'S SCHEME

To analyze the security of Khan et al.'s scheme, we assume that an attacker can obtain the secret values stored in the smart card by monitoring the power consumption [12-13] and intercept the messages communicating between the user and the server.

A. Password Guessing Attack

Generally, most of users tend to select a password that is easily remembered for his convenience. Hence, this password is potentially vulnerable to password guessing attack. With the extracted secret value $\{L, r\}$ in the legal user's smart card and the intercepted messages $\{C_1, T_i\}$, the attacker can easily guess the legal user's password pw_i in the following steps.

- PA1. In the login phase, the attacker computes $C_1=h(T_i \parallel J)=h(T_i \parallel (L \oplus (h(r \parallel pw_i^*))))$, where pw_i^* is a guessed password.
- PA2. The attacker verifies a correctness of user's password pw_i^* .
- PA3. The attacker repeats the step PA1 and PA2 by replacing another guessed password pw_i^* until the legal user's password pw_i is found.

Finally, the attacker can obtain the correct user's password pw_i . With the guessed password, the attacker can easily perform forgery attack and session key attack.

B. Forgery Attack

With the extracted secret values $\{L, y, r\}$ in the legal user's smart card, the guessed password pw_i^* in Section 3.1, and the intercepted message $\{AID_i, T_i, d\}$, the attacker A_i can easily perform forgery attack in the following steps.

- FA1. A_i computes $RPW^*=h(r \parallel pw_i^*)$, $J^*=L \oplus RPW^*$ and $C_1^*=h(T_i^* \parallel J^*)$, where T_i^* is a current timestamp.
- FA2. A_i computes $ID_i^*=AID_i \oplus h(y \parallel T_i \parallel d)$ and computes $AID_i^*=ID_i^* \oplus h(y \parallel T_i^* \parallel d^*)$, where a random number d^* is generated by the attacker.
- FA3. Then, A_i sends the forged login request message $\{AID_i^*, T_i^*, d^*, C_1^*\}$ to the remote server S .
- FA4. Upon receiving the forged login message, S verifies the validity of T_i^* . S computes $ID_i^{**}=AID_i^* \oplus h(y \parallel T_i^* \parallel d^*)$ if it is valid, and verifies the validity of the user's ID^{**} .

FA5. S checks the value of N in the database and computes $IDU^*=(ID_i^{**} \parallel N)$.
 FA6. S computes $J^*=h(x \parallel IDU^*)$ and checks whether $h(T_i^* \parallel J^*)=C_1^*$ or not. If they are equal, the forged login request message is accepted and the attacker is authenticated by the remote server.

The very secret value $\{L, y, r\}$, and the guessed password pw_i^* can be also utilized in the server masquerading attack in the following steps.

FA7. A_i computes $C_2^*=h(C_1^* \oplus J^* \oplus T_s^*)$, and then sends the forged reply message $\{C_2^*, T_s^*\}$ to U_i , where T_s^* is a current timestamp.
 FA8. Upon receiving the forged reply message, U_i verifies the validity of T_s^* .
 FA9. U_i checks whether $h(C_1 \oplus J \oplus T_s^*)=C_2^*$ or not. If they are equal, the forged reply message is accepted and the attacker is authenticated by the user.

C. User Anonymity

With the extracted secret values $\{y\}$ from the legal user's smart card and the intercepted message $\{AID_i, T_i, d\}$ communicating between the user and the server, the attacker can easily obtain the legal user's identity. As you notice, the attacker can compute $ID_i=AID_i \oplus h(y \parallel T_i \parallel d)$, and then the attacker can identify the personal trying to login into the server. Hence we can see that Khan et al.'s scheme does not provide the user anonymity.

D. Session Key Agreement

Generally, the session key agreement in the authentication scheme is provided for security of messages communicating between the server and the user. In Khan et al.'s scheme, the attacker can compute the one-time session key $S_k=h(C_2 \oplus J)$ if the attacker can obtain the secret value $\{L, r\}$ stored in the legal user's smart card, with the guessed password pw_i^* , and the intercepted message $\{C_2\}$ communicating between the server and the user. Hence, we can see that Khan et al.'s scheme does not provide the session key agreement.

IV. THE IMPROVED SCHEME

In this section, we propose an improved scheme to enhance Khan et al.'s scheme. The improved scheme is divided into three phases: registration phase, login phase and authentication phase. The login and authentication phase in the improved scheme are illustrated in Fig. 1.

A. Registration Phase

Before performing the registration phase, the remote server S has to generate a large prime p and finds an integer g which is a primitive element in $GF(p)$. Then, a user U_i registers to S in the following steps.

R1. U_i submits his identity ID_i and password information $RPW=h(r \parallel pw_i)$ to the server over a secure channel, where a random number r is chosen by U_i .
 R2. S computes the following equations, where $IDU=(ID_i \parallel N)$ and N is a number of re-registering in the system.

$$\begin{aligned} J &= h(x \parallel IDU) \\ m &= J \oplus h(x) \\ L &= m \oplus RPW \end{aligned}$$

R3. S issues the smart card to U_i , which contains values $\{L, J, y, h()\}$ over a secure channel.
 R4. U_i securely stores random number r in the smart card and need not to remember its value.

B. Login Phase

This phase works whenever the user U_i wants to login to the remote server S. The smart card performs the following steps.

L1. U_i inserts his smart card into a card reader, and inputs his identity ID_i with his password pw_i .
 L2. The smart card generates a random number r_c and computes $R_c=g^{r_c} \text{ mod } p$.
 L3. Then, the smart card computes the following equations, where T_i is a current timestamp.

$$\begin{aligned} m &= L \oplus RPW \\ C_1 &= J \oplus m \oplus R_c \\ AID_i &= ID_i \oplus h(y \parallel T_i \parallel R_c) \end{aligned}$$

L4. The user sends a login request message $\{AID_i, C_1, J, T_i\}$ to the server.

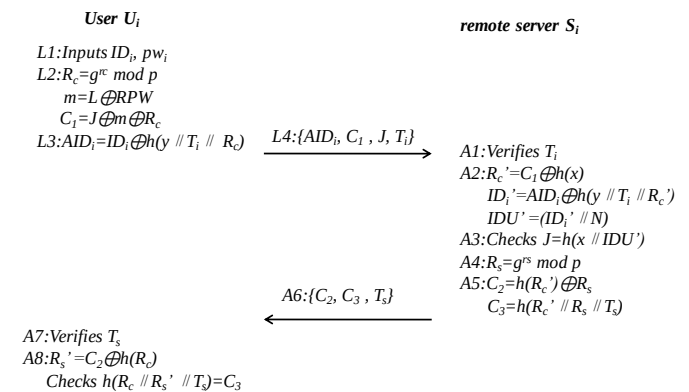


Fig. 1. Login phase and authentication phase

C. Authentication Phase

This phase works whenever the remote server S received the user's login request message. Upon receiving the message from the user, the server performs the following steps to authenticate each other.

- A1. The server verifies the timestamp T_i with the current time T' . If $(T' - T_i) \leq \Delta T$, the server accepts the login request, where ΔT denotes the expected valid time interval for transmission delay.
- A2. The server computes $R_c' = C_1 \oplus h(x)$, $ID_i' = AID_i \oplus h(y \parallel T_i \parallel R_c')$, and $IDU' = (ID' \parallel N)$.
- A3. The server checks whether $J = h(x \parallel IDU')$ or not. If they are equal, the server authenticates the user.
- A4. The server generates a random number r_s and computes $R_s = g^{r_s} \bmod p$.
- A5. Then, the server computes $C_2 = h(R_c') \oplus R_s$ and $C_3 = h(R_c' \oplus R_s \oplus T_s)$, where T_s is a current timestamp.
- A6. The server sends a mutual authentication message $\{C_2, C_3, T_s\}$ to the user.
- A7. Upon receiving the message, the smart card verifies the timestamp T_s with the current time T'' . If $(T'' - T_s) \leq \Delta T$, the smart card accepts the message, where ΔT denotes the expected valid time interval for transmission delay.
- A8. The smart card computes $R_s' = C_2 \oplus h(R_c)$, and then checks whether $C_3 = h(R_c \oplus R_s' \oplus T_s)$ or not. If they are equal, the user authenticates the server.

After achieving mutual authentication, the server and the user can generate the session key $SK = (R_s')^{rc} = (R_c')^{rs} = g^{rs \cdot rc} \bmod p$ each other for secrecy communication.

V. SECURITY ANALYSIS OF THE IMPROVED SCHEME

In this section, we provide the security analysis of the improved scheme based on the secure hash function and the discrete logarithm problem.

A. Security Analysis

To analyze the security of the improved scheme, we assume that an attacker could obtain the values stored in a user's smart card by monitoring the power consumption [12-13] and the intercepted message communicating between the user and the server. Here, we only discuss forgery attack, password guessing attack, user anonymity, and session key agreement.

Forgery attack

To impersonate the legal user, an attacker attempts to make a forged login request message which can be authenticated to the server. However, the attacker cannot impersonate the user by forging the login request message, because the attacker cannot compute the forged login request message $\{AID_{ia}, C_{1a}\}$ without knowing the server's secret value x , the user's password pw_i and random number R_c . Thus, the attacker has no chance to login by launching a user impersonation attack.

Also, the attacker cannot masquerade as the server by forging the reply message, because the attacker does not compute $\{C_{2a}, C_{3a}\}$ without knowing the server's secret value x , and random numbers R_c, R_s . Hence, the attacker cannot masquerade as the legal server to the user by launching a server masquerading attack. Thus, the attacker cannot masquerade as the legal server to the user by launching a server masquerading attack.

Password guessing attack

With the extracted secret values $\{L, J, y, r\}$ in the legal user's smart card and the intercepted messages $\{C_1\}$ between the user and the server, the attacker may attempt to guess the user's password pw_i by computing $L = m \oplus RPW$ in the registration phase or $C_1 = J \oplus m \oplus R_c$ in the login phase. However, the attacker cannot guess the user's password pw_i , because the attacker does not know the secret value x kept by the server. Thus, the improved scheme is secure for the off-line password guessing attack.

User anonymity

With the extracted secret values $\{L, J, y, r\}$ from the legal user's smart card and the intercepted message $\{AID_i, T_i\}$ communicating between the user and the server, the attacker may attempt to get the legal user's identity ID_i by computing $AID_i = ID_i \oplus h(y \parallel T_i \parallel R_c)$ in the login phase. However, the attacker cannot get the legal user's identity ID_i , because the attacker does not know the random parameter $R_c (= g^{rc} \bmod p)$ generated by the smart card. Thus, we can see that the improved scheme does not provide the user anonymity.

Session key agreement

With the extracted secret values in the legal user's smart card and the intercepted messages communicating between the user and the server, the attacker may attempt to compute the one-time session key SK . However, the attacker cannot generate the one-time session key $SK (= g^{rs \cdot rc} \bmod p)$ without knowing the random number R_s generated by the user and the random number R_c generated by the user. Thus, we can see that the improved scheme provides the session key agreement securely.

B. Comparison of the Improved Scheme with the Related Schemes

The security analysis of the related scheme and the improved scheme is summarized in TABLE II. The improved scheme is relatively more secure than the related scheme. In addition, the improved scheme provides the user anonymity and the session key agreement.

TABLE II
COMPARISON OF THE IMPROVED SCHEME WITH THE RELATED SCHEMES

Security Features	Wang et al.'s scheme	Khan et al.'s scheme	Improved scheme
forgery attack	possible	possible	impossible
password guessing attack	possible	possible	impossible
user anonymity	not provided	not provided	provided
session key agreement	not provided	provided	provided

VI. CONCLUSIONS

In this paper, we analyzed the security of Khan et al.'s scheme, which scheme is not secure against the various attacks and does not provide the user anonymity. Also, we

proposed the improved scheme to overcome the user forgery attack, the password guessing attack, and to provide the user anonymity and the session key agreement, even if the secret information stored in the smart card is revealed. As a result, the improved scheme is relatively more secure than the related schemes in terms of the security.

ACKNOWLEDGMENT

Younghwa An thanks the anonymous reviewers for their valuable comments.

REFERENCES

- [1] H.M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, 2000.
- [2] S.T. Wu, B.C. Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards," *Computers & Security*, Vol. 22, No. 6, pp. 457-550, 2003.
- [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, pp. 612-614, 2004.
- [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, pp. 629-631, 2004.
- [5] W.C. Ku, S.T. Chang, "Impersonation Attack on a Dynamic ID-based Remote User Authentication Scheme Using Smart Cards," *IEICE Transactions on Communication*, E88-B(5), pp. 2165-216, 2005.
- [6] H.Y. Chien, C.H. Chen, "A Remote Authentication Scheme Preserving User Anonymity," *International Conference on AINA 2*, pp. 245-248, 2005.
- [7] I. Liao, C.C. Lee and M.S. Hwang, "Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme," *International Conference on Next Generation Web Services Practices 2005*, pp. 437-440, 2005.
- [8] 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.
- [9] Y.Y. Wang, J.Y. Kiu, F.X. Xiao and J. Dan, "A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme," *Computer Communications*, Vol. 32, pp. 583-585, 2009.
- [10] 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.
- [11] M.K. Khan, S.K. Kim and K. Alghathbar, "Cryptanalysis and Security Enhancement of a 'More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme,'" *Computer Communications*, Vol.34, No. 3, pp. 305-309, 2011.
- [12] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," *Proceedings of Advances in Cryptology*, pp. 388-397, 1999.
- [13] 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.



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. His major research interests include information security and network security.