Security Enhancements of Smart Card-Based Remote User Password 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, Gyounggi-do, 446-702, Korea
yhan@kangnam.ac.kr

Abstract—**Smart card-based user authentication schemes have been proposed recently to improve the security drawbacks in user authentication scheme. Li et al., in 2013, proposed an enhanced smart card-based remote user password authentication scheme which can withstand the security drawbacks of Chen et al.'s scheme. In this paper, we show that Li et al.'s scheme is vulnerable to user impersonation attack, server masquerading attack, password guessing attack and does not provide mutual authentication between the user and the server. Also, we propose the enhanced scheme with session key agreement to overcome the security drawbacks of Li et al.'s scheme, even if the secret values stored in the smart card is revealed. As a result, the enhanced scheme is relatively more secure than the related scheme in terms of security.**

Keywords—**Authentication, User Impersonation Attack, Server Masquerading Attack, Password Guessing Attack, Session Key Agreement**

I. INTRODUCTION

With rapid development of the Internet technology, user authentication scheme in e-commerce and m-commerce has been becoming one of important security issues. Remote user authentication scheme is a mechanism to authenticate remote user over insecure communication network. 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 enhanced schemes [1-7] have been proposed for secure communication between the user and the server.

Generally speaking, an ideal smart card-based password authentication scheme [8] should withstand various attacks, such as denial of service attack, forgery attack, parallel attack, password guessing attack, replay attack, stolen smart-card attack, stolen verifier attack, insider attack, etc. Besides, an ideal smart card-based password authentication scheme should satisfy some security requirements, such as no verification table, freely chosen password, no password reveal, mutual authentication, session key agreement, forward secrecy, user anonymity, efficiency for wrong password login, etc. Unfortunately, none of the existing password authentication schemes can withstand the above attacks and satisfy all the security requirements.

In 2012, Chen et al. [9] proposed robust smart card-based remote user password authentication scheme which can withstand the security drawbacks of Sood et al.'s scheme and Song scheme. They claimed that their scheme not only keeps the original requirement but also achieves mutual authentication. But, in 2013, Li et al. [10] pointed out that Chen et al.' scheme does not provide forward secrecy and prompt detection of the wrong password. Then, Li et al. proposed an enhanced smart card-based remote user password authentication scheme which can withstand the security drawbacks of Chen et al.'s scheme.

In this paper, we analyze the security of Li et al.'s remote user authentication scheme, and we show that Li et al.'s remote user authentication scheme is still vulnerable to the various attacks such as password guessing attack, user impersonation attack, server masquerading attack, etc. and does not provide mutual authentication between the user and the server.

To analyze the security analysis of Li et al.'s remote user authentication scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [11-12] and intercept messages communicating between the user and the server. Also, we assume that an attacker may possess the capabilities [4] 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.

Obviously, 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

*This research was supported by Kangnam University Research Grants.(2013)

user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

The remainder of this paper is organized as follows. In Section II, we briefly review Li et al.'s authentication scheme. In Section III, we describe security analysis of Li et al.'s scheme. The enhanced 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 Li et al.'s Scheme

In 2013, Li et al. [10] proposed an enhanced smart card based remote user password authentication scheme. For a detailed security analysis, we first review Li et al.'s scheme.

The scheme is composed of three phases: the registration phase, the login phase, and the authentication phase. The notations used in this paper are defined in TABLE I.

In order to initialize the scheme, the server S selects large prime number p and q such that p=2q+1, then S chooses the master key $x \in Z_q$ and an appropriate one-way hash function h().

TABLE I
Notation and Definition

Notation	Description
U_i	User i
S	Server
ID_i	Identity of the user i
pw_i	Password of the user i
BIO_i	Biometric template of the user i
h()	A secure hash function
x	A master secret key kept by the server
$A \| B$	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 PW_i to S via a secure channel.

R2. S computes the security parameters, where x is a secret value selected by the server.

$$A_i = h(ID_i \| PW_i)^{PW_i} \bmod p$$

$$B_i = h(ID_i)^{x+PW_i} \bmod p$$

R3. S stores (A_i, B_i, h(), p, q) on a smart card and issues it to the user via a secure channel.

B. Login Phase

When the user U_i wants to login the remote server S, the user has to perform the following steps. The login and authentication phase are illustrated in Figure1.

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

L2. The smart card computes $A_i^* = h(ID_i \| PW_i)^{PW_i} \bmod p$. If A_i^* equals A_i, the smart card computes the following equations, where $a \in_R Z_q^*$ is a random number selected by the smart card and T_i is the current timestamp.

$$C_i = B_i / h(ID_i)^{PW_i} \bmod p$$

$$D_i = h(ID_i)^a \bmod p$$

$$M_i = h(ID_i \| C_i \| D_i \| T_i)$$

L3. The smart card sends the login request message {ID_i, D_i, M_i, T_i} to S.

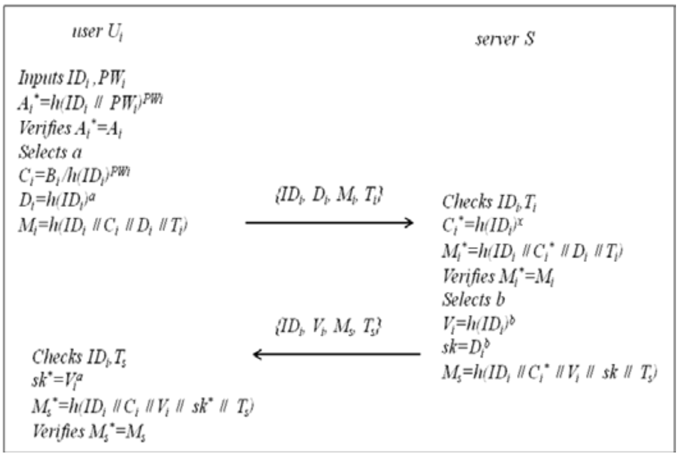
user U_i
server S
Inputs ID_i ,PW_i
$A_i^*=h(ID_i \, // \, PW_i)^{PW_i}$
Verifies $A_i^*=A_i$
Selects a
$C_i=B_i/h(ID_i)^{PWi}$
$D_i=h(ID_i)^a$
$M_i=h(ID_i \, // C_i \, // D_i \, // T_i)$
{ID_i, D_i, M_i, T_i}
Checks ID_i,T_i
$C_i^*=h(ID_i)^x$
$M_i^*=h(ID_i \, // C_i^* \, // D_i \, // T_i)$
Verifies $M_i^*=M_i$
Selects b
$V_i=h(ID_i)^b$
$sk=D_i^b$
$M_s=h(ID_i \, // C_i^* \, // V_i \, // \, sk \, // \, T_s)$
{ID_i, V_i, M_s, T_s}
Checks ID_i,T_s
$sk^*=V_i^a$
$M_s^*=h(ID_i \, // C_i \, // V_i \, // \, sk^* \, // \, T_s)$
Verifies $M_s^*=M_s$

Figure 1. Login phase and authentication phase of Li et al.'s scheme

C. Authentication Phase

After receiving the login request message, the remote server S has to perform the following steps.

A1. S checks the ID_i and T_i.

A2. If they are valid, S computes the following equations.

$$C_i^* = h(ID_i)^x \bmod p$$

$$M_i^* = h(ID_i \| C_i^* \| D_i \| T_i)$$

A3. S verifies whether $M_i^* = M_i$ or not. If they are equal, S computes the following equations, where $b \in_R Z_q^*$ is a random number selected by the server and T_s is the current timestamp.

$$V_i = h(ID_i)^b \bmod p$$

$$sk = D_i^b \bmod p$$

$$M_s = h(ID_i \| C_i^* \| V_i \| sk \| T_s)$$

A4. Then, S sends the mutual authentication message {ID_i, V_i, M_s, T_s} to U_i.

A5. After receiving the message, the smart card checks the ID_i and T_s.

A6. If they are valid, the smart card computes the following equations.

$$sk^* = V_i^a \bmod p$$

$$M_s^* = h(ID_i \| C_i \| V_i \| sk^* \| T_s)$$

A7. The smart card verifies whether $M_s^* = M_s$ or not. If they are equal, the server S is authenticated by the user U_i.

Therefore, the user U_i and the server S can get the shared session key $sk = h(ID_i)^{ab} \bmod p$.

III. Security Analysis of Li et al.'s Scheme

In this section, we analyze the security drawbacks of Li et al.'s scheme. To analyze, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [11-12] and intercept 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, these passwords are potentially vulnerable to password guessing attack. If an attacker can extract the secret value (A_i) illegally from the legal user's smart card by monitoring the power consumption, the attacker can easily find out the legal user's password by performing the password guessing attack, in which each guess PW_i^* for PW_i can be verified as the following steps.

PA1. The attacker computes the secret parameter $A_i^*= h(ID_i \| PW_i^*)^{PWi^*}$ mod p from the registration phase.

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

PA3. The attacker repeats the above steps until a correct password PW_i^* is found.

Thus, the attacker can get the legal user's password easily by performing the password guessing attack. Consequently, the attacker can successfully impersonate the legal user and masquerade the legal server with the guessed user's password PW_i^*.

B. User Impersonation Attack

With the guessed user's password PW_i^* and the secret value (B_i) extracted from the user's smart card illegally, the attacker can perform the user impersonation attack as the following steps. The procedure of the user impersonation attack is illustrated in Figure 2.

UA1. The attacker computes the following equations, where $a^* \in_R Z_q^*$ is a random number selected by the attacker and T_i^* is a timestamp.

$$C_i^*=B_i/h(ID_i)^{PWi^*} \bmod p$$
$$D_i^*=h(ID_i)^{a^*} \bmod p$$
$$M_i^*=h(ID_i \| C_i^* \| D_i^* \| T_i^*)$$

UA2. Then, the attacker sends the forged login request message $\{ID_i, D_i^*, M_i^*, T_i^*\}$ to the server S.

UA3. Upon receiving the forged login request message, S checks the ID_i and T_i^*. If they are valid, S computes $C_i=h(ID_i)^x$ and $M_i^{**}=h(ID_i \| C_i \| D_i^* \| T_i^*)$.

UA4. S verifies whether $M_i^*=M_i^{**}$ or not. If they are equal, the attacker is authenticated as the legal user U_i by the server S.

C. Server Masquerading Attack

With the guessed user's password PW_i^*, the secret value (B_i) extracted from the user's smart card and the intercepted message (D_i) illegally, the attacker can perform the server masquerading attack as the following steps. The procedure of the server masquerading attack is illustrated in Figure 2.

SA1. The attacker computes the following equations, where $b^* \in_R Z_q^*$ is a random number selected by the attacker and T_s^* is a timestamp.

$$C_i^*=B_i/h(ID_i)^{PWi^*} \bmod p$$
$$V_i^*=h(ID_i)^{b^*} \bmod p$$
$$sk^*=D_i^{b^*} \bmod p$$
$$M_s^*=h(ID_i \| C_i^* \| V_i^* \| sk^* \| T_s^*)$$

SA2. Then, the attacker sends the forged mutual authentication message $\{ID_i, V_i^*, M_s^*, T_s^*\}$ to the user U_i.

SA3. Upon receiving the forged mutual authentication message, the smart card checks the ID_i and T_s^*. If they are valid, the smart card computes the following equations.

$$sk^{**}=V_i^{*a} \bmod p$$
$$M_s^{**}=h(ID_i \| C_i \| V_i^* \| sk^{**} \| T_s^*)$$

SA4. The smart card verifies whether $M_s^*=M_s^{**}$ or not. If they are equal, the attacker is authenticated as the legal server S by the user U_i.

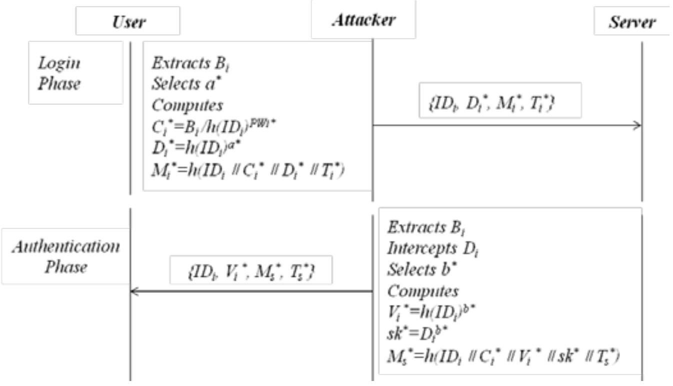

Figure 2. User impersonation attack and server masquerading attack

D. Mutual Authentication and Session Key Agreement

Generally, if an 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, Li et al.'s scheme fails to provide mutual authentication as described the above subsection 3.B, 3.C. Namely, if the attacker can obtain the secret value (B_i) from the legal user's smart card by monitoring the power consumption and intercept the message (D_i) communicating between the user and the server, the attacker can get the forged login request message easily by computing $C_i^*=B_i/h(ID_i)^{PWi^*}$ mod p, $D_i^*=h(ID_i)^{a^*}$ mod p, and $M_i^*=h(ID_i \| C_i^* \| D_i^* \| T_i^*)$ in the login phase. Receiving the forged login request message, the server authenticates the attacker as a legal user. Also, the server makes the mutual authentication message easily by computing $C_i=h(ID_i)^x$, $V_i=h(ID_i)^b$, $sk=D_i^{*b}$, and $M_s=h(ID_i \| C_i \| V_i \| sk \| T_s)$ in the authentication phase. With the mutual authentication message, the attacker can get a shared session key for communication between the server and the user.

As a result of security analysis, we can see that Li et al.'s scheme is still vulnerable to the various attacks and fails to provide the mutual authentication.

IV. The Enhanced Scheme

In this section, we propose an enhanced scheme to improve the security drawbacks of Li et al.'s scheme. The enhanced scheme is divided into three phases: registration phase, login phase and authentication phase. In order to initialize the scheme, the server S selects large prime number p and q such that p=2q+1, then S chooses the master key $x \in Z_q$ and an appropriate one-way hash function h().

A. 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 password information $h(PW_i \oplus K)$ to S via a secure channel. Also, U_i submits his biometric information $h(BIO_i \oplus K)$ via the specific device to S, where K is a random number chosen by the user.

$$A_i = h(PW_i \oplus K) \oplus h(BIO_i \oplus K)$$
$$B_i = h(ID_i)^{x + h(PW_i \oplus K)} \bmod p$$

R3. S stores $\{ID_i, A_i, B_i, h(), p, q\}$ on a smart card and issues it to the user via a secure channel.

R4. Then, U_i stores K on his smart card.

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. The login phase is shown in Fig. 3.

L1. U_i inserts his smart card into a card reader and inputs his ID_i and PW_i. Also, U_i inputs his biometric BIO_i on the specific device.

L2. The smart card computes $A^* = h(PW_i \oplus K) \oplus h(BIO_i \oplus K)$. If the computed value A^* matches A stored in the smart card, the smart card performs the remaining steps of the login phase.

L3. The smart card computes the following equations, where $a \in_R Z_q^*$ is a random number selected by the smart card and T_i is the current timestamp.

$$C_i = B_i / h(ID_i)^{h(PW_i \oplus K)} \bmod p$$
$$D_i = h(ID_i)^a \bmod p$$
$$M_i = h(ID_i \parallel C_i \parallel D_i \parallel T_i)$$

L4. The smart card sends a login request message $\{ID_i, D_i, M_i, T_i\}$ to the server.

A. 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. The authentication phase is shown in Figure 3.

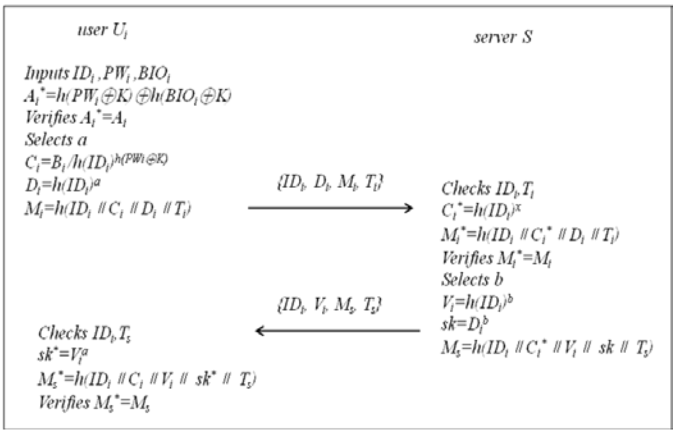
user U_i
server S
Inputs ID_i ,PW_i ,BIO_i
$A_i^* = h(PW_i \oplus K) \oplus h(BIO_i \oplus K)$
Verifies $A_i^* = A_i$
Selects a
$C_i = B_i / h(ID_i)^{h(PWi \oplus K)}$
$D_i = h(ID_i)^a$
$M_i = h(ID_i \parallel C_i \parallel D_i \parallel T_i)$
$\{ID_i, D_i, M_i, T_i\}$
Checks ID_i,T_i
$C_i^* = h(ID_i)^x$
$M_i^* = h(ID_i \parallel C_i^* \parallel D_i \parallel T_i)$
Verifies $M_i^* = M_i$
Selects b
$V_i = h(ID_i)^b$
$sk = D_i^b$
$M_s = h(ID_i \parallel C_i^* \parallel V_i \parallel sk \parallel T_s)$
$\{ID_i, V_i, M_s, T_s\}$
Checks ID_i,T_s
$sk^* = V_i^a$
$M_s^* = h(ID_i \parallel C_i \parallel V_i \parallel sk^* \parallel T_s)$
Verifies $M_s^* = M_s$

Figure 3. Login phase and authentication phase

A1. S checks the ID_i and T_i.

A2. If they are valid, S computes the following equations.

$$C_i^* = h(ID_i)^x \bmod p$$
$$M_i^* = h(ID_i \parallel C_i^* \parallel D_i \parallel T_i)$$

A3. S verifies whether the computed value M_i^* matches M_i or not. If they are equal, S computes the following equations, where $b \in_R Z_q^*$ is a random number selected by the server and T_s is the current timestamp.

$$V_i = h(ID_i)^b \bmod p$$
$$sk = D_i^b \bmod p$$
$$M_s = h(ID_i \parallel C_i^* \parallel V_i \parallel sk \parallel T_s)$$

A4. Then, S sends the mutual authentication message $\{ID_i, V_i, M_s, T_s\}$ to U_i.

A5. After receiving the message, the smart card checks the ID_i and T_s.

A6. If they are valid, the smart card computes the following equations.

$$sk^* = V_i^b \bmod p$$
$$M_s^* = h(ID_i \parallel C_i \parallel V_i \parallel sk^* \parallel T_s)$$

A7. The smart card verifies whether $M_s^* = M_s$ or not. If they are equal, the server S is authenticated by the user U_i.

After achieving mutual authentication, the server and the user can generate the shared session key $sk = h(ID_i)^{ab} \bmod p$ each other for secrecy communication.

V. Security Analysis of the Enhanced Scheme

In this section, we provide the security analysis of the enhanced scheme and compare it with the related schemes.

A. Security Analysis

To analyze the security of the enhanced scheme, we assume that an attacker can get the secret information stored in a user's smart card by monitoring the power consumption [11-12] and the intercepted message communicating between the user and the server.

User impersonation attack

In order to perform the user impersonation attack, the attacker has to make a login request massage {ID_i, D_i, M_i, T_i} which can pass the authentication by the server. However, the attacker cannot impersonate as the user by forging the login request massage, because the attacker has no way to get (C_i, D_i, M_i) without knowing the server's secret key x, the user's password PW_i and random number a selected by the user. Hence, the enhanced scheme can resist user impersonation attack.

Server masquerading attack

In order to perform the server masquerading attack, the attacker has to make a mutual authentication massage {ID_i, V_i, M_s, T_s} which can pass the authentication by the user. However, the attacker cannot masquerade as the server by forging the mutual authentication massage, because the attacker has no way to get (C_i^*, V_i, M_s) without knowing the server's secret key x and random number b selected by the server. Hence, the enhanced scheme can resist server masquerading attack.

Password guessing attack

With the extracted secret values (A_i, B_i, K) in the legal user's smart card and the intercepted messages {M_i} between the user and the server, the attacker may attempt to guess the user's password PW_i by computing $A_i=h(PW_i \oplus K) \oplus h(BIO_i \oplus K)$, $B_i=h(ID_i)^{x+h(PW_i \oplus K)}$ mod p in the registration phase or $M_i=h(ID_i \parallel C_i \parallel D_i \parallel T_i)$ in the login phase. However, the attacker cannot guess the user's password PW_i, because the attacker does not know the secret key x kept by the server and the user's biometric template BIO_i. Hence, the enhanced scheme can resist off-line password guessing attack.

Detection of wrong password

In the enhanced scheme, the smart card can verify the validity of the user's password promptly in the login phase. When the user inputs his identity ID_i and password PW_i, the smart card performs the password verify phase as a first step by computing $A^*=h(PW_i \oplus K) \oplus h(BIO_i \oplus K)$. If A^* does not equal A stored in the smart card, the smart card terminates the session because the user inputs a wrong password. If A^* equals A, the smart card performs the remaining steps of the login phase. Hence, the enhanced scheme can detect the wrong password promptly by the smart card at the beginning of the login phase.

Mutual Authentication

As previously described in cases such as the user impersonation attack and the server masquerading attack, the enhanced scheme provides mutual authentication between the user and the server. Namely, even if the attacker can extract the secret values (A_i, B_i, K) in the legal user's smart card and intercept the messages communicating between the user and the server, the user can be authenticated by the server and the server can be authenticated by the user, because the attacker cannot get the forged messages in each phase without knowing the server's secret key x and the selected random number a, b. Hence, the enhanced scheme provides mutual authentication securely between the user and the server.

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 shared session key sk. However, the attacker cannot get the one-time shared session key sk($=h(ID_i)^{ab}$ mod p) without knowing the random number a selected by the user and the random number b selected by the server. Hence, the enhanced scheme provides the one-time shared session key securely.

B. Comparison of the Enhanced Scheme with the Related Schemes

The security analysis of the related schemes and the enhanced scheme is summarized in TABLE II. The enhanced scheme is relatively more secure than the related schemes. Also, the enhanced scheme provides mutual authentication and session key agreement.

TABLE II
COMPARISON OF THE ENHANCED SCHEME WITH THE RELATED SCHEMES

Security Features	Chen et al.'s scheme	Li et al.'s scheme	Enhanced scheme
User impersonation attack	possible	possible	impossible
Server masquerading attack	possible	possible	impossible
Password guessing attack	possible	possible	impossible
Detection of wrong password	not provide	provide	provide
Mutual authentication	not provide	not provide	provide
Session key agreement	not provide	not provide	provide

VI. CONCLUSIONS

In 2013, Li et al. proposed an enhanced smart card-based remote user password authentication scheme which can withstand the forgery attack, the stolen smart card attack, the replay attack, etc. In this paper, we provide the security analysis of Li et al.'s scheme. And we verified that Li et al.'s scheme is still vulnerable to the user impersonation attack, the server masquerading attack, and the password guessing attack and does not provide the mutual authentication between the user and the server. Also, we propose the enhanced scheme with session key agreement to overcome the security drawbacks of Li et al.'s scheme, even if the secret values stored in the smart card is revealed. As a result, the enhanced scheme is relatively more secure than the related schemes in terms of security.

ACKNOWLEDGMENT

Younghwa An thanks the anonymous reviewers for their valuable comments.

REFERENCES

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

[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, pp. 612-614, 2004.

[3] 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.

[4] J. Xu, W.T. Zhu and D.G. Feng, “An Improved Smart Card-Based Password Authentication Scheme with Provable Security,” *Computer Standard and Interfaces*, Vol. 31(4), pp. 723-8, 2009

[5] 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, pp. 1-5, 2010.

[6] R. Song, “Advanced Smart Card-Based Password Authentication Protocol,” *Computer Standard and Interfaces*, Vol. 32(5), pp. 321-5, 2010.

[7] A.K. Das, “Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards,” *IET Information Security*, Vol.5, Iss. 3, pp. 541-552, 2011.

[8] R. Madhusudhan and R.C. Mittal, “Dynamic ID-Based Remote User Password Authentication Scheme using Smart Cards: A Review,” *Journal of Network and Computer Applications*, Vol. 35, pp. 1235-1248, 2012.

[9] B.L. Chen, W.C. Kuo and L.C. Wuu, “Robust Smart Card-Based Remote User Password Authentication Scheme,” *International Journal of Communication Systems*, http://dx.doi.org/10.1002/dac.2368, 2012.

[10] X. Li, J. Niu, M.K. Khan and J. Liao, “An Enhanced Smart Card-Based Remote User Password Authentication Scheme,” Journal of Network and Computer Applications, vol. 36, pp. 1365-1371, 2013.

[11] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", *Proceedings of Advances in Cryptology*, pp. 388-397, 1999.

[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, 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.