Security Enhancements of a Password-Based Mutual Authentication Scheme Using Smart Cards

Younghwa An

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

Abstract

Password-based authentication scheme is one of the efficient authentication mechanics to protect resources from unauthorized access. Chang-Lee, in 2008, proposed a password-based mutual authentication scheme to overcome the security drawbacks of Wu-Chieu's scheme. In this paper, we have shown that Chang-Lee's scheme is vulnerable to various attacks known by literatures. Also we proposed an improved scheme to overcome the security drawbacks of Chang-Lee's scheme. As a result of analysis, the proposed scheme not only withstands the various attacks, such as the user impersonation attack, the server masquerading, the man-in-the-middle attack, the off-line password guessing, the insider attack, but also provides mutual authentication between the user and the server. At the same time, the proposed scheme is more efficient than the related schemes in terms of the computational complexities.

Keywords: *Mutual Authentication, User Authentication Attack, Server Masquerading Attack, Password Guessing Attack*

1. Introduction

Password-based authentication scheme is one of the convenient and efficient authentication mechanics. This mechanism has been widely adopted for various kinds of authentication applications which are remote login, on-line banking, access control of restricted area, etc. However, numerous vulnerabilities have been disclosed in the authentication scheme due to careless password management and sophisticated attack techniques. Several improved schemes [1-10] for remote user authentication schemes using smart card have been proposed.

In 2000, Sun [1] proposed an elaborate remote user authentication scheme using a smart card with the advantages of a no password table. But the scheme also has the disadvantage in that the password of the user is assigned by the remote server. Wu-Chieu [2], in 2003, proposed a user friendly remote user authentication scheme with smart cards to improve the drawbacks of Sun's scheme which required the assignment of un-human lengthy passwords. However, in 2004, Yang-Wang [4] pointed out that Wu-Chieu's scheme is vulnerable to off-line password guessing and forgery attack. In 2008, Chang-Lee [7] proposed a friendly password-based mutual authentication scheme to avoid the security weakness of Wu-Chieu's scheme. They asserted that their scheme was secure against forgery, off-line password guessing, and replay attack, and provided mutual authentication between the user and the remote server.

In this paper, we analyze the security weaknesses of Chang-Lee's scheme and we have shown that Chang-Lee's scheme is still insecure against user impersonation, server masquerading, off-line password guessing, and insider attack. To analyze the security of Chang-Lee's scheme, we assume that an attacker can access a user's smart card and extract

the secret information 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. And we propose an improved scheme providing mutual authentication to overcome the security weaknesses of Chang-Lee's scheme, while preserving all their merits, even if the secret information stored in the smart card is revealed. 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.

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

This paper is organized as follows. In section 2, we briefly reviews Chang-Lee's scheme. In section 3, we describe the security weaknesses of Chang-Lee's scheme. The improved scheme is presented in section 4, and its security analysis and performance evaluations are given in section 5. Finally, the conclusions are made in section 6.

2. Reviews of Chang-Lee's Scheme

In 2008, Chang-Lee [7] proposed a friendly password mutual authentication scheme for remote login network systems. This scheme is divided into three phases: registration phase, login phase, and authentication phase. The notations used throughout this paper are in table 1.

Table 1. Notations used in this Paper

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	A secret key maintained by the server
A ‖ B	Concatenates A with B
A⊕B	XOR operates A with B

2.1. Registration Phase

This phase works whenever a user U_i wants to register initially or re-register to the remote server *S*. The registration phase is illustrated in Figure 1.

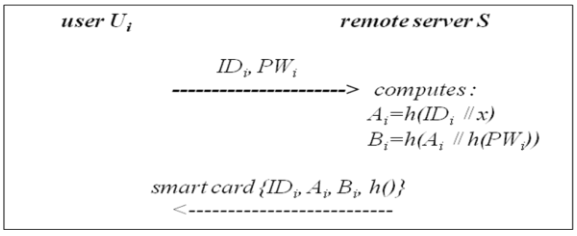


Figure 1. Registration Phase of Chang-Lee's Scheme

R1. A user submits his identity ID_i and password PW_i to the server through a secure channel.

R2. The server computes $A_i=h(ID_i \| x)$ and $B_i=h(A_i \| h(PW_i))$, where x is a secret key of server.

R3. The server issues the smart card to the user through a secure channel, where the smart card contains $\{ID_i, A_i, B_i, h()\}$.

2.2. Login Phase

This phase works whenever the user U_i wants to login to the remote server S. The login and authentication phase are illustrated in Figure 2.

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

L2. The smart card computes $B_i^*=h(A_i \| h(PW_i^*))$, $C_1=h(B_i \oplus T_1)$ and $C_2= B_i^* \oplus h(A_i \oplus T_1)$, where T_1 is the current time stamp.

L3. The user sends a message $m_1=\{ID_i, C_1, C_2, T_1\}$ to the server.

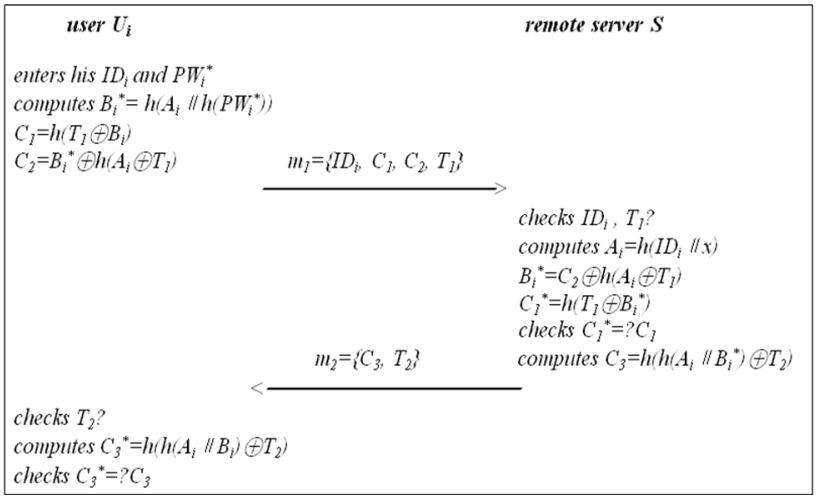


Figure 2. Login and Authentication Phase of Chang-Lee's Scheme

2.3. Authentication Phase

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

A1. The server checks the validity of the user's identity ID_i, and then verifies the validity of the time interval between T' and T_1, where T' is the time of receiving m_1 at the remote server.

A2. The server computes $A_i=h(ID_i \| x)$, $B_i^*=C_2 \oplus h(A_i \oplus T_1)$ and $C_1^*=h(B_i^* \oplus T_1)$.

A3. The server checks whether $C_1^*=C_1$ or not. If they are equal, the user's login request is accepted.

A4. The server sends a message $m_2=\{C_3, T_2\}$, where $C_3=h(h(A_i \| B_i^*) \oplus T_2)$ and T_2 is the current time stamp.

A5. Upon receiving the message, the smart card verifies the validity of the time interval between T'' and T_2, where T'' is the time of receiving m_2 at the user.

A6. The smart card computes $C_3^*=h(h(A_i \| B_i) \oplus T_2)$, and then checks whether $C_3^*= C_3$ or not. If they are equal, the server is authenticated to the user.

3. Security Weaknesses of Chang-Lee's Scheme

In this section, we analyze the security drawbacks of Chang-Lee's scheme, such as user impersonation attack, server masquerading attack, password guessing attack, insider attack, and mutual authentication. To analyze the security of Chang-Lee's scheme, we assume that an attacker can access a user's smart card and extract the secret information 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.

3.1. User Impersonation Attack

As described above, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means and intercept the message $m_1=\{ID_i, C_1, C_2, T_1\}$ communicating between the user and the server. The procedure for the user impersonation attack occurs in the following steps. They are illustrated in Figure 3.

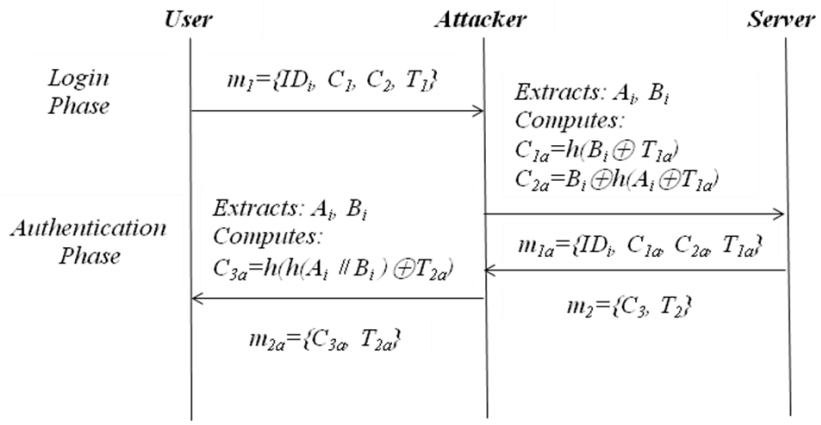


Figure 3. User Impersonation Attack and Server Masquerading Attack

Step1. In the login phase, the attacker computes easily $C_{1a}=h(B_i \oplus T_{1a})$ and $C_{2a}=B_i \oplus h(A_i \oplus T_{1a})$ by extracting the secret values (A_i, B_i), where T_{1a} is the current time stamp.

Step2. Then, the attacker sends the forged message $m_{1a}=\{ID_i, C_{1a}, C_{2a}, T_{1a}\}$ to the remote server *S*.

Step3. Upon receiving the message, the remote server checks the validity of ID_i and verifies the validity of the time interval. If it holds, the remote server will be convinced the message m_{1a} sent from the user by verifying whether $C_1^*=C_{1a}$ or not. And then the remote server makes the reply massage $m_2=\{C_3, T_2\}$ by computing $C_3=h(h(A_i \| B_i^*) \oplus T_2)$ in the authentication phase.

3.2. Server Masquerading Attack

As described above, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means and intercepts the message $m_2=\{C_3, T_2\}$ communicating between the user and the server. The procedure for the server masquerading attack is as following steps. They are illustrated in Figure 3.

Step1. In the authentication phase, the attacker computes easily $C_{3a}=h(h(A_i \| B_i) \oplus T_{2a})$ extracting the secret values (A_i, B_i), where T_{2a} is the current time stamp.

Step2. Then, the attacker sends the forged message $m_{2a}=\{C_{3a}, T_{2a}\}$ to the user.

Step3. Upon receiving the message, the user verifies the validity of the time interval. If it holds, the user will be convinced the message m_{2a} sent from the remote server by verifying whether $C_3^*=C_{3a}$ or not.

3.3. Password Guessing Attack

As described above, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means. Now, the attacker can easily find out the user's password PW_i by employing the off-line password guessing attack, in which each guess PW_i^* for PW_i can be verified by the following steps.

Step1. The attacker computes the parameter $B_i^*=h(A_i \| h(PW_i^*))$ from the registration phase.

Step2. The attacker verifies the correctness of PW_i^* by checking $B_i^*=B_i$.

Step3. The attacker repeats the above steps until a correct password PW_i^* is found. Finally, the attacker can derive the correct user's password PW_i.

Thus, the attacker can perform the off-line password guessing attack, and can successfully impersonate the legal user with the guessed user password.

3.4. Insider Attack

In the registration phase, if the user's password PW_i is revealed to the server, the insider of the server may directly obtain PW_i. Thus the insider as an attacker can impersonate as the legal user to access the user's other accounts in other server if the user uses the same password for the other accounts. Therefore, Chang-Lee's scheme is not secure for the insider attack.

3.5. Mutual Authentication

As described above, in attacks such as the user impersonation attack and the server masquerading attack, Chang et al.'s scheme fails to provide the mutual authentication between the user and the remote server. Namely, if the attacker can extract the secret values (A_i, B_i) from the legal user's smart card illegally by some means and intercept the messages communicating between the user and the server, the attacker can impersonate the legal user easily by computing the equations $C_{1a}=h(B_i \oplus T_{1a})$ and $C_{2a}=B_i \oplus h(A_i \oplus T_{1a})$. Also, the attacker can masquerade the legal remote server easily by computing the equation $C_{3a}=h(h(A_i \| B_i) \oplus T_{2a})$.

4. The Proposed Scheme

In this section, we propose an improved Chang-Lee's scheme which not only can withstand the various attacks, but also provide mutual authentication between the user and the server. The proposed scheme is divided into three phases: registration phase, login phase and authentication phase.

4.1. Registration Phase

This phase works whenever a user U_i initially wants to register or re-register to the remote server S. The registration phase is illustrated in Figure 4.

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

R2. The server computes $A_i=h(ID_i \oplus x)$ and $B_i=A_i \oplus h(b \oplus PW_i))$, where x is a secret key of server.

R3.The server issues the smart card to the user through a secure channel, where the smart card contains $\{ID_i, B_i, h()\}$.

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

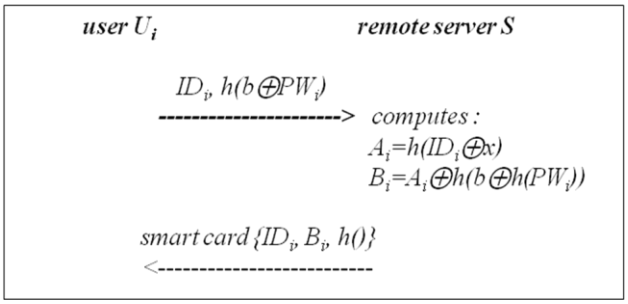


Figure 4. Registration Phase of the Proposed Scheme

4.2. Login Phase

This phase works whenever the user U_i wants to login to the remote server S. The login and authentication phase are illustrated in Figure 5.

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

L2.The smart card computes $A_i=B_i \oplus h(b \oplus PW_i)$, $C_1=h(A_i \oplus R)$ and $C_2=R \oplus h(A_i \oplus T_1)$, where T_1 is the current time stamp and R is a random nonce generated by the smart card.

L3.The user sends a message $\{ID_i, C_1, C_2, T_1\}$ to the server.

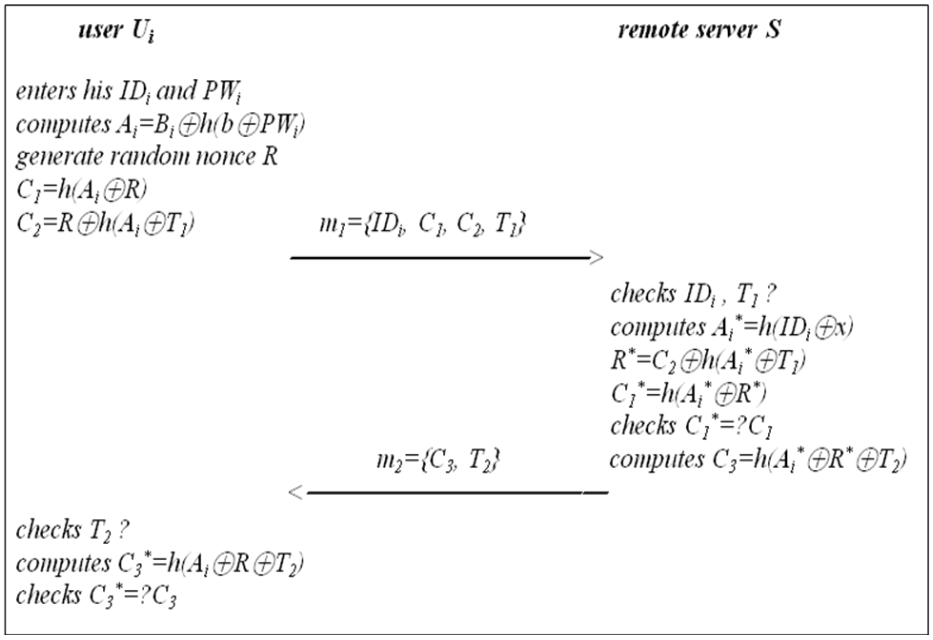


Figure 5. Login Phase and Authentication Phase of the Proposed Scheme

4.3. Authentication Phase

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

A1. The server checks the validity of ID_i, and then verifies the time stamp T_1 with the current time T'. If $(T'-T_1) \leq \Delta T$, the server accepts the login request, where ΔT denotes the expected valid time interval for transmission delay.

A2. The server computes $A_i^* = h(ID_i \oplus x)$, $R^* = C_2 \oplus h(A_i^* \oplus T_1)$, and $C_1^* = h(A_i^* \oplus R^*)$.

A3. The server checks whether $C_1^* = C_1$ or not. If they are equal, the user's login request is accepted.

A4. The server computes $C_3 = h(A_i^* \oplus R^* \oplus T_2)$, where T_2 is the current time stamp, and then sends a message $\{C_3, T_2\}$ to the user.

A5. Upon receiving the message, the smart card verifies the time stamp T_2 with the current time T''. If $(T''-T_2) \leq \Delta T$, and then the smart card computes $C_3^* = h(A_i \oplus R \oplus T_2)$.

A6. The smart card checks whether $C_3^* = C_3$ or not. If they are equal, the server is authenticated to the user and allowed to access the smart card.

5. Security Analysis and Performance Evaluations of the Proposed Scheme

In this section, we will analyze the proposed scheme in terms of security. Also we will evaluate the performance of the proposed scheme in terms of computation.

5.1. Security Analysis

To analyze the security of the proposed scheme, we assume that can access a user's smart card, extract the values stored in the smart card by some means [11-13], and intercept the messages communicating between the user and the server. Here, we only discuss the user impersonation attack, the server masquerading attack, the man-in-the-middle attack, the off-line password guessing attack, the insider attack and mutual authentication.

5.1.1. User impersonation 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 massage, because the attacker cannot compute the forged message C_{1a}, C_{2a} without knowing the remote server's secret value *x*, the user's password PW_i and random nonce *R*. Hence, the attacker has no chance to login by launching a user impersonation attack.

5.1.2. Server masquerading attack: To masquerade as the legal server, an attacker attempts to make the forged reply massage which can be masqueraded to the user when receiving the user's login request message. However, the attacker cannot masquerade as the server by forging the reply massage, because the attacker does not compute C_{3a} without knowing the remote server's secret value *x*, the user's password PW_i and random nonce *R*. Hence, the attacker cannot masquerade as the legal server to the user by launching a server masquerading attack.

5.1.3. Man-in-the-middle attack: To perform the man-in-the-middle attack, an attacker attempts to make the forged massages $\{ID_i, C_{1a}, C_{2a}, T_{1a}\}$ with the legitimate message $\{ID_i, C_1, C_2, T_1\}$ intercepted in the login phase and $\{C_{3a}, T_{2a}\}$ with the legitimate message $\{C_3, T_2\}$ intercepted in the authentication phase. However, the attacker cannot make the forged massages, because the attacker is not able to compute these forged messages without knowing the remote server's secret value *x*, the user's password PW_i and random nonce *R*, even if the

attacker can obtain the secret values stored in the user's smart card[11-13]. Hence, the attacker cannot perform the man-in-the-middle attack while communicating between the server and the user.

5.1.3. Password guessing attack: The attacker can extract the secret values (A_i, B_i) from the legal user's smart card by some means. Then the attacker attempts to derive the user's password PW_i using $B_i=h(A_i \oplus h(PW_i))$ in the registration phase. However, the attacker cannot guess the user's password PW_i using the secret values extracted from the legal user's smart card, because the attacker does not know the remote server's secret value x. Therefore, the proposed scheme is secure for the off-line password guessing attack.

5.1.4. Insider attack: In the registration phase, if the user's password PW_i is revealed to the server, insider attack of the server may directly obtain PW_i and impersonate as the user to access user's other accounts in other server if the user use the same password for the other accounts. Therefore, the proposed scheme is secure for the insider attack, because this scheme asks the user to submit $h(b \oplus PW_i)$ instead of a PW_i to the server.

5.1.5. Mutual authentication: As previously described in cases such as the user impersonation attack and the server masquerading attack, the proposed scheme provides mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret information 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 each phase without knowing the remote server's secret value x, the user's password PW_i and random nonce R.

5.1.6. Comparison of the related schemes: The security analysis of the related scheme and the proposed scheme is summarized in Table 2. The proposed scheme is relatively more secure than Chang-Lee's scheme. In addition, the proposed scheme provides mutual authentication between the user and the server.

Table 2. Comparison of the Related Scheme and the Proposed Scheme

security features	Sun's scheme [1]	Wu-Chieu's scheme [2]	Chang-Lee's scheme [7]	the proposed scheme
user impersonation attack	possible	possible	possible	impossible
sever masquerading attack	*not provided	*not provided	possible	impossible
man-in-the-middle attack	*not provided	*not provided	possible	impossible
password guessing attack	possible	possible	possible	impossible
insider attack	possible	possible	possible	impossible
mutual authentication	*not provided	*not provided	impossible	possible

5.2. Performance Evaluations

In this section, we evaluate the efficiency of the proposed scheme in terms of the computational complexities by comparing it with the related scheme. In Table 3, it is clear that the proposed scheme is more efficient than Chang-Lee's scheme.

Table 3. Comparison of the Related Scheme and the Proposed Scheme

phase	Sun's scheme	Wu-Chieu's scheme	Chang-Lee's scheme	the proposed scheme
registration phase	1TH	2TH+1TM+1TE	3TH	2TH+3TX
login phase	1TH+1TX	2TH+1TX+1TM+ 1TE	4TH+3TX	3TH+5TX
authentication phase	2TH+1TX	1TH+1TX	7TH+5TX	5TH+8TX

*TH: the time for performing a one-way hash function, TX: the time for performing a exclusive-OR computation, TE: the time for performing a exponent computation, TM: the time for performing a multiplication

6. Conclusions

In this paper, we analyzed the security of Chang-Lee's scheme. Although Chang-Lee's scheme improved the drawbacks of Wu-Chieu's scheme, we have shown that Chang-Lee's scheme is vulnerable to forgery attack and password guessing attack, etc. And we proposed the improved scheme to overcome the security drawbacks of Chang-Lee's scheme, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, the proposed scheme not only withstands the various attacks, such as the user impersonation attack, the server masquerading, the man-in-the-middle attack, the off-line password guessing, the insider attack, and but also provides mutual authentication between the user and the server. At the same time, the proposed scheme is more efficient than the related schemes in terms of the computational complexities.

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 and B. C. Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards", Computers & Security, Vol. 22, No. 6, pp. 457-550 **(2003)**.

[3] 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)**.

[4] C. C. Yang and R.C. Wang, "Cryptanalysis of a User Friendly Remote Authentication Scheme with Smart Cards", Computers & Security, Vol. 223, No. 5, pp. 425-427 **(2004)**.

[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, pp.1-8 **(2008)**.

[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, pp.73-80 **(2008)**.

[7] C. C. Chang and C. Y. Lee, "A Friendly Password Mutual Authentication Scheme for Remote Login Network Systems", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 1, pp. 59-63 **(2008)**.

[8] 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)**.

[9] C. C. Chang, S. C. Chang and Y. W. Lai, "An Improved Biometrics-based User Authentication Scheme without Concurrency System", International Journal of Intelligent Information Processing, Vol.1, No.1, pp. 41-49 **(2010)**.

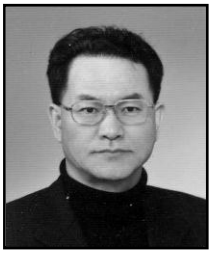
[10] D. S. Wang and J. P. Li, "A Novel Mutual Authentication Scheme Based on Fingerprint Biometric and Nonce Using Smart Cards", International Journal of Security and its Applications, Vol. 5, No. 4, pp.1-12 **(2011)**.

[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)**.

[13] E. Brier, C. Clavier and F. Oliver, "Correlation power analysis with a leakage model", Lecture Notes in Computer Science, Vol. 3156, pp. 135-152 **(2004)**.

Author



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