International Journal of Future Generation Communication and Networking
Vol. 2, No. 4, December, 2009

Weaknesses and Improvements of a One-time Password Authentication Scheme

Mijin Kim, Byunghee Lee, Seungjoo Kim, and Dongho Won

School of Information and Communication Engineering,
Sungkyunkwan University, Suwon 440-746, Republic of Korea
{mjkim, bhlee, skim, dhwon}@security.re.kr

Abstract

Authentication of communicating entities and confidentiality of transmitted data are fundamental procedures to establish secure communications over public insecure networks. Recently, many researchers proposed a variety of authentication schemes to confirm legitimate users. Among the authentication schemes, a one-time password authentication scheme requires less computation and considers the limitations of mobile devices. The purpose of a one-time password authentication is to make it more difficult to gain unauthorized access to restricted resources. This paper discusses the security of Kuo-Lee's one-time password authentication scheme. Kuo-Lee proposed to solve the security problem based on Tsuji-Shimizu's one-time password authentication scheme. It was claimed that their proposed scheme could withstand a replay attack, a theft attack and a modification attack. Therefore, the attacker cannot successfully impersonate the user to log into the system. However, contrary to the claim, Kuo-Lee's scheme does not achieve its main security goal to authenticate communicating entities. We show that Kuo-Lee's scheme is still insecure under a modification attack, a replay attack and an impersonation attack, in which any attacker can violate the authentication goal of the scheme without intercepting any transmitted message. We also propose a scheme that resolves the security flaws found in Kuo-Lee's scheme.

Keywords: *One-time password, authentication scheme, impersonation attack.*

1. Introduction

Mobile devices are designed to help users access the servers of service providers. They process tasks such as, stock trading, product purchases, product information collection, and banking. Once the services are available to the users, authentication is applied to verify the identities of users. However, most current authentication methods used in M-commerce are designed for wired networks and require high computation costs, making them unsuited to wireless environments. A one-time password authentication scheme uses less computation and considers the limitations of mobile devices. The purpose of a one-time password is to make it more difficult to gain unauthorized access to restricted resources. Traditionally static passwords can be more easily accessed by an unauthorized intruder given sufficient attempts and time. This risk can be greatly reduced by constantly altering the password. There are basically three types of one-time passwords. The first uses a mathematical algorithm to generate a new password based on the previous password. The second is based on time-synchronization between the authentication server and the user providing the password. The third uses a mathematical algorithm, but the new password is based on a challenge and a counter. A one-time password system generates a series of passwords that are used to log on to a specific system. Once one of the passwords is used, it cannot be used again. The login

system will always expect a new one-time password at the next login.

Lamport [1] introduced the first one-time password authentication scheme. This initial work has been followed by a number of subsequent improvements [2-9]. Of theses schemes, SAS-2 [7] suffers from a stolen-verifier attack; an attacker who has stolen user verifiers from the server can impersonate legitimate users. ROSI [8] suffers from a theft attack; an attacker who has stolen the server's secret can impersonate legitimate users. In 2004, Tsuji-Shimizu proposed 2GR [9] to eliminate a stolen-verifier attack on SAS-2 and a theft attack on ROSI. Although Tsuji-Shimizu claimed that under 2GR an attacker who has stolen the verifiers from the server cannot impersonate a legitimate user, Lin-Hung showed that the 2GR scheme is vulnerable to an impersonation attack, in which any attacker can masquerade as a legitimate user, without stealing the verifiers [10]. Kuo-Lee pointed out that the 2GR is insecure under a modification attack and proposed an improved scheme to enhance the security of the one-time password authentication scheme in 2007 [11]. However, we found in this paper Kuo-Lee's scheme is vulnerable to modification, replay and impersonation attacks.

The remainder of this paper is organized as follows: In Section 2, we review Kuo-Lee's one-time password authentication scheme. We present security weaknesses of Kuo-Lee's scheme in Section 3. In Section 4, we propose an enhanced scheme, and analyze the security in Section 5. Finally, we conclude this work in Section 6.

2. Review of Kuo-Lee's scheme

The following notation is listed below with the descriptions to facilitate future reference.

- *U*: a legitimate user
- *S*: a server
- *A*: an attacker
- *ID*: *U*'s identity
- *PW*: *U*'s password
- *h*: a one-way hash function
- *N*: a random number
- $\oplus$: an exclusive-or operation
- $U \rightarrow S$: transmitting *U* to *S* over an unauthenticated channel

Kuo-Lee's scheme consists of two phases: the registration phase and the authentication phase. The registration phase is performed only once, when a new user registers with the server; while the authentication phase is executed every time a user wants to gain access to the server. We describe these two phases as follows.

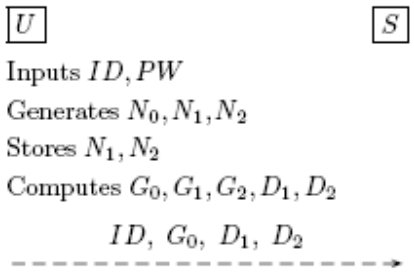

Figure 1. Registration phase of Kuo-Lee's scheme

2.1 Registration phase

Figure 1 shows the initial registration phase of the Kuo-Lee's scheme where a dashed line indicates an authenticated channel and more detailed description follows:

R1. A user *U* inputs <*ID, PW*> and generates three random numbers <N_0, N_1, N_2>. Then *U* stores <N_1, N_2>and calculates <G_0,G_1,G_2, D_1, $D2$> by using the following equations:

$$G_0 = h(ID, PW, N_0),$$
$$G_1 = h(ID, PW, N_1),$$
$$G_2 = h(ID, PW, N_2),$$
$$D_1 = h(G_0, G_1),$$
$$D_2 = h(G_1, G_2).$$

R2. *U* sends < *ID*, G_0, D_1, D_2> to *S*.
R3. *S* stores the received message < *ID*, G_0, D_1, D_2>.

2.2 Authentication phase

In order to log into the system, *U* executes the *i*th authentication session of Kuo-Lee's scheme. When *U* finishes the (*i* - 1)th login session of the scheme, <N_i, N_{i+1}> is stored in *U* and <*ID*, G_{i-1}, D_i, D_{i+1}> is stored in *S*. Figure 2 shows the *ith* authentication phase of Kuo-Lee's scheme. The detailed description of the *i*th authentication phase is as follows:

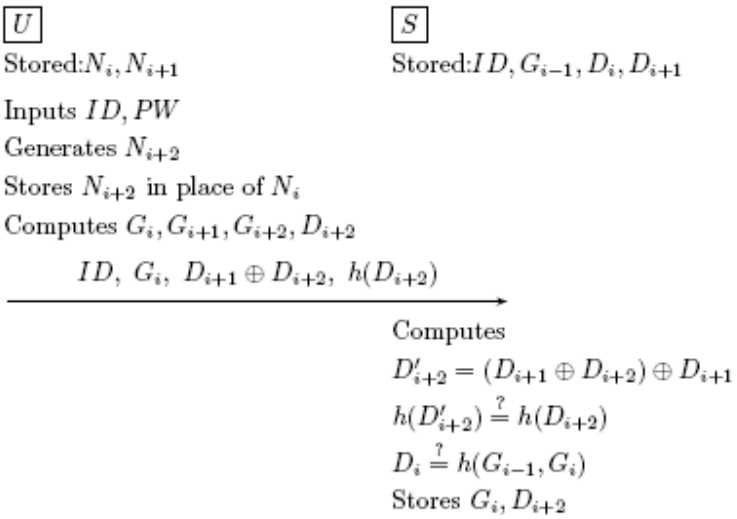

Figure 2. Authentication phase of Kuo-Lee's scheme

A1. *U* first inputs <*ID, PW*>. Next he generates a new random number N_{i+2} and computes <G_i, G_{i+1}, G_{i+2}, D_{i+2}> where

$$G_i = h(ID, PW, N_i),$$
$$G_{i+1} = h(ID, PW, N_{i+1}),$$
$$G_{i+2} = h(ID, PW, N_{i+2}),$$

$$D_{i+2} = h(G_{i+1}, G_{i+2}).$$

Then U stores $<N_{i+1}, N_{i+2}>$ instead of $<N_i, N_{i+1}>$.

A2. U sends $<ID, Gi, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$ to S.

A3. S first computes $D'_{i+2} = (D_{i+1} \oplus D_{i+2}) \oplus D_{i+1}$ and checks if $h(D'_{i+2})$ is equal to $h(D_{i+2})$ when he received the message $<ID, G_i, D_{i+1} \oplus D_{i+2}; h(D_{i+2})>$. If $h(D'_{i+2}) = h(D_{i+2})$ then S computes $D'_i = h(G_{i-1}, G_i)$ using the stored G_{i-1} and the received G_i, and checks if D'_i is equal to the stored D_i. If they match, U is authenticated, and then S stores $<ID, Gi, D_{i+1}, D_{i+2}>$ in place of $<ID, G_{i-1}, D_i, D_{i+1}>$. Otherwise, S rejects U's login.

3. Attacks on Kuo-Lee's scheme

In 2006, Lin-Hung pointed out the vulnerability of the 2GR scheme to an impersonation attack [10]. Lin-Hung's approach can be directly applied to Kuo-Lee's scheme that provides unilateral authentication. Thus the attacker can apply server spoofing on Kuo-Lee's scheme. Kuo-Lee argued that their proposed scheme can withstand replay, theft and modification attacks. Therefore, the attacker cannot impersonate user U to log into the system. However, under our investigation, Kuo-Lee's scheme cannot work successfully.

We deduce the security weakness of Kuo-Lee's scheme, in which a situation could arise whereby the original message could have been suppressed and thus did not arrive at its destination; only the replay message arrives. We show this by mounting three attacks, a modification attack, a replay attack and an impersonation attack, on Kuo-Lee's scheme. The scenarios of our attacks on Kuo-Lee's scheme are as follows.

3.1. Modification attack and replay attack

1. $U \rightarrow A$ $<ID, Gi, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$

(a) In the ith authentication session, the user U sends $<ID, Gi, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$ to the server.
(b) Since the user does not authenticate the server in Kuo-Lee's scheme, we assume that using server spoofing, an attacker masquerades as the server to receive the transmitted message from the user, and accepts this login connection.
(c) The attacker cannot provide subsequent service to the user, from user U's viewpoint, the ith authentication is accomplished but the service is interrupted.
(d) Now the user is with $<N_{i+1}, N_{i+2}>$ while the server is still with $<ID, G_{i-1}, D_i, D_{i+1}>$.

2. $U \rightarrow A$ $<ID, G_{i+1}, D_{i+2} \oplus D_{i+3}, h(D_{i+3})>$

(a) In the $(i+1)$th authentication session, when the user U sends $<ID, G_{i+1}, D_{i+2} \oplus D_{i+3}, h(D_{i+3})>$ to the server, the attacker intercepts the transmitted message.
(b) The attacker records G_{i+1}.

3. $A \rightarrow S$ $<ID, G_i, D_{i+1} \oplus D'_{i+2}, h(D'_{i+2})>$

(a) A forwards the server $<ID, G_i, D_{i+1} \oplus D'_{i+2}, h(D'_{i+2})>$ in which the attacker chooses a random number G'_{i+2} and calculates $D'_{i+2} = h(G_{i+1}, G'_{i+2})$.
(b) After receiving the data from the attacker, server S calculates $D''_{i+2} = (D_{i+1} \oplus D'_{i+2}) \oplus$

D_{i+1}, using the received $D_{i+1} \oplus D'_{i+2}$ and stored D_{i+1}.
(c) Then S compares $h(D''_{i+2})$ with received $h(D'_{i+2})$.
(d) If they are equal, then the server will pass the authentication check and update user's verifier as $<ID, G_i, D_{i+1}, D'_{i+2}>$. From user U's viewpoint, the (i+1)th authentication is accomplished and service is supplied.

Therefore, if an attacker intercepted the transmitted message at the ith login and replayed it to gain an access, the attack can work. Kuo-Lee claimed that their proposed scheme can withstand modification and replay attacks. However, this turns out to be untrue.

3.2. Impersonation attack

After the modification attack and replay attack, attacker A is able to impersonate U to log into the system. The attack proceeds as follows:

1. $A \rightarrow S$ $<ID, G_{i+1}, D'_{i+2} \oplus D'_{i+3}, h(D'_{i+3})>$

(a) In the (i+2)th authentication session, A chooses a random number G'_{i+3} and calculates $D'_{i+3} = h(G'_{i+2}, G'_{i+3})$.
(b) A sends $<ID, G_{i+1}, D'_{i+2} \oplus D'_{i+3}, h(D'_{i+3})>$ to S, in which the G_{i+1} is recorded at step 3.1 2(b).
(c) After receiving the message from A, S calculates $D''_{i+3} = (D'_{i+2} \oplus D'_{i+3}) \oplus D'_{i+2}$, using the received $D'_{i+2} \oplus D'_{i+3}$ and stored D'_{i+2}.
(d) If $h(D''_{i+3})$ is equal to the received $h(D'_{i+3})$, S calculates $D'_{i+1} = h(G_i, G_{i+1})$ using the stored G_i and received G_{i+1}.
(e) S compares D'_{i+1} with the stored D_{i+1}. If they are equal, S will pass the authentication check.
(f) S updates U's verifier as $<ID, G_{i+1}, D'_{i+2}, D'_{i+3}>$.

2. $A \rightarrow S$ $<ID, G'_{i+2}, D'_{i+3} \oplus D'_{i+4}, h(D'_{i+4})>$

(a) In the (i+2)th authentication session, A chooses a random number G'_{i+4} and calculates $D'_{i+4} = h(G'_{i+3}, G'_{i+4})$.
(b) A sends $<ID, G'_{i+2}, D'_{i+3} \oplus D'_{i+4}, h(D'_{i+4})>$ to S.
(c) After receiving the message from the attacker, S calculates $D''_{i+4} = (D'_{i+3} \oplus D'_{i+4}) \oplus D'_{i+3}$, using the received $D'_{i+3} \oplus D'_{i+4}$ and stored D'_{i+3}.
(d) If $h(D''_{i+4})$ is equal to the received $h(D'_{i+4})$, S calculates $D''_{i+2} = h(G_{i+1}, G'_{i+2})$, using the stored G_{i+1} and received G'_{i+2}.
(e) S compares D''_{i+2} with the stored D'_{i+2}. If they are equal, S will pass the authentication check.
(f) S updates U's verifier as $<ID, G'_{i+2}, D'_{i+3}, D'_{i+4}>$.

In this authentication phase, the attacker chooses all the numbers $<G'_{i+2}, D'_{i+3}, D'_{i+4}>$. Therefore, from now on A can impersonate the U without intercepting any transmitted message. Hence, the attacker can successfully impersonate the user to log into the system.

4. Proposed scheme

We propose an enhanced scheme to achieve security against the presented attacks. The

scheme allows the communicating entities to protect their communications in the authentication phase. Only U and S have a shared key K in order to secure the scheme. The proposed scheme has two phases: registration phase and authentication phase.

4.1. Registration Phase

The registration phase is performed only once, when a new user registers with the server.

R1. U inputs $<ID, PW>$

1. U generates three random numbers $<N_0, N_1, N_2>$.
2. U stores $<N_1, N_2>$.
3. U calculates $<G_0, G_1, G_2, D_1, D2>$ by using the following equations:

$$G_0 = h(ID, PW, N_0),$$
$$G_1 = h(ID, PW, N_1),$$
$$G_2 = h(ID, PW, N_2),$$
$$D_1 = h(G_0, G_1),$$
$$D_2 = h(G_1, G_2).$$

R2. $U \rightarrow S$ $< ID, G_0, G_1, D_1, D_2>$
R3. S stores the received message $< ID, G_0, G_1, D_1, D_2>$.

4.2. Authentication phase

In the authentication phase, the user is requesting the ith service. When U finishes the $(i-1)$th authentication session of the scheme, $<N_i, N_{i+1}>$ is stored in U and $<ID, G_{i-1}, G_i, D_i, D_{i+1}>$ is stored in S. The detailed description of the ith enhanced authentication phase is as follows:

A1. $U \rightarrow S$ login request

1. U inputs $<ID, PW>$.
2. U send a login request to S.

A2. $S \rightarrow U$ $E_K(ID \oplus T_S \oplus i)$

1. S computes $<ID \oplus T_S \oplus i>$, where T_S is S's current timestamp and i is the current session number.
2. S encrypts $<ID \oplus T_S \oplus i>$, using the shared key K.
3. S sends $E_K(ID \oplus T_S \oplus i)$ to U.

A3. $U \rightarrow S$ $<E_K(ID \oplus T_U \oplus i), G_{i-1} \oplus G_i \oplus G_{i+1}, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$

1. U decrypts $E_K(ID \oplus T_S \oplus i)$.
2. U checks $(T_U - T_S) \geq \Delta T$. If $(T_U - T_S) \geq \Delta T$, U quits the login request, where ΔT is the expected valid time interval.
3. Otherwise, U generates a new random number N_{i+2}.
4. U computes $<G_i, G_{i+1}, G_{i+2}, D_{i+2}>$, where

$G_i = h(ID, PW, N_i)$,
$G_{i+1} = h(ID, PW, N_{i+1})$,
$G_{i+2} = h(ID, PW, N_{i+2})$,
$D_{i+2} = h(G_{i+1}, G_{i+2})$.

5. U stores $<N_{i+1},N_{i+2}>$ instead of $<Ni,N_{i+1}>$.
6. U computes $<ID \oplus T_U \oplus i>$, where T_U is U's current timestamp and i is the current session number.
7. U encrypts $<ID \oplus T_U \oplus i>$ using the shared key K.
8. U sends $<E_K(ID \oplus T_U \oplus i), G_{i-1} \oplus G_i \oplus G_{i+1}, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$ to S.

A4. S receives $<E_K(ID \oplus T_U \oplus i), G_{i-1} \oplus G_i \oplus G_{i+1}, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$

1. S decrypts $E_K(ID \oplus T_U \oplus i)$.
2. S checks $(T_U\text{-}T_S) \geq \Delta T$. If $(T_U\text{-}T_S) \geq \Delta T$, S rejects the login request, where ΔT is the expected valid time interval.
3. Otherwise, S computes $D'_{i+2} = (D_{i+1} \oplus D_{i+2}) \oplus D_{i+1}$.
4. S checks if $h(D'_{i+2})$ is equal to $h(D_{i+2})$.
5. If $h(D'_{i+2}) = h(D_{i+2})$, then S obtains $G_{i+1} = (G_{i-1} \oplus G_i \oplus G_{i+1}) \oplus G_{i-1} \oplus G_i$.
6. S computes $D'_{i+1} = h(G_i,G_{i+1})$, using the stored G_i and the obtained G_{i+1}.
7. S checks if D'_{i+1} is equal to the stored D_{i+1}.
8. If they are equal, U is authenticated, and then S stores $<ID,G_i,G_{i+1},D_{i+1},D_{i+2}>$ in place of $<ID, G_{i-1},G_i, D_i, D_{i+1}>$.
9. Otherwise, S rejects U's login.

Table 1. Security comparisons of related authentication schemes

	2GR	Kuo-Lee's Scheme	Proposed Scheme
Modification Attack	X	X	O
Replay Attack	O	X	O
Impersonation Attack	O	X	O

O means the scheme is not vulnerable to the attack. X means the scheme is vulnerable to the attack.

5. Security analysis

In this section, we briefly demonstrates that our proposed scheme is secure against a modification attack, a replay attack and an impersonation attack. In Table 1, we summarize the security comparisons of our proposed scheme and the related authentication schemes.

5.1 Resistance to Modification Attack

In the ith authentication session, when the user sends $<E_K(ID \oplus T_U \oplus i), G_{i-1} \oplus G_i \oplus G_{i+1}, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$ to the server, we assume that the attacker intercepts the transmitted message and tries to modify the message. In our proposed scheme, the attacker is unable to modify the message $<E_K(ID \oplus T_U \oplus i), G_{i-1} \oplus G_i \oplus G_{i+1}, D_{i+1} \oplus D_{i+2}, h(D_{i+2})>$, since the attacker cannot compute $<D_{i+1} = h(G_i,G_{i+1})>$ or $<D_{i+2} = h(G_{i+1},G_{i+2})>$ even if A eavesdropped on previous messages. Therefore, our modification attack is no longer valid against our enhanced scheme.

5.2 Resistance to Replay Attack and Impersonation Attack

We assume that an attacker eavesdrops on U's message $<D_{i+1} = h(G_i,G_{i+1})>$ or $<D_{i+2} = h(G_{i+1},G_{i+2})>$ in the ith authentication session, and sends the message to S for the $(i+1)$th authentication session. Obviously, S rejects the message, because U's timestamp and session number are always updated in every authentication session and S checks the valid time interval of ΔT and the session number. Therefore, our scheme protects U and S from replay attack. Due to the failure of the modification and replay attacks, our impersonation attack is no longer valid against our enhanced scheme.

6. Conclusion

We presented the security weakness of Kuo-Lee's one-time password authentication scheme [11]. Kuo-Lee claimed that their proposed scheme could withstand a replay attack, a theft attack and a modification attack; therefore, the attacker could not successfully impersonate the user to log into the system. However, contrary to the claim, our security investigation showed that Kuo-Lee's scheme does not achieve its main security goal to authenticate communicating entities. The failure of Kuo-Lee's scheme to achieve authentication was clear using three attacks: modification, replay and impersonation attacks, on the scheme. We proposed an enhancement to the original scheme to secure the scheme, remedying these problems.

References

[1] L. Lamport, “Password authentication with insecure communication”, Commun. ACM, vol.24, no.11, pp. 770-772, Nov. 1981.
[2] A. Shimizu, “A dynamic password authentication method by oneway function”, System and Computers in Japan, vol.22, no.7, pp. 32-40, July 1991.
[3] N.M. Haller, “The S/KEY (TM) one-time password system”, Proc. Internet Society Symposium on Network and Distributed System Security, pp. 151-158, Feb. 1994.
[4] A. Shimizu, T. Horioka, and H. Inagaki, “A password authentication method for contents communication on the Internet”, IEICE Trans. Commun., vol. E81-B, no.8, pp. 1666-1673, Aug. 1998.
[5] M. Sandirigama, A. Shimizu, and M.T. Noda, “Simple and Secure password authentication protocol (SAS)”, IEICE Trans. Commun., vol. E83-B, no. 6, pp. 1363-1365, June 2000.
[6] C.L. Lin, H.M. Sun, and T. Hwang, “Attack and solutions on strong-password authentication”, IEICE Trans. Commun., vol. E84-B, no.9, pp. 2622-2627, Sept. 2001.
[7] T. Tsuji, T. Kamioka, and A. Shimizu, “Simple and Secure password authentication protocol, ver.2 (SAS-2)”, IEICE Technical Report, OIS 2002-30, Sept. 2002.
[8] H.Y. Chien, J.K. Jan, “Robust and simple authentication protocol”, Comput. J., vol.46, no.2, pp. 193-201, Feb. 2003.
[9] T. Tsuji, A. Shimizu, “One-time password authentication protocol against theft attacks”, IEICE Trans. on Commun., vol.E87-B, no.3, pp. 523-529, Mar. 2004.
[10] C.L. Lin, C.P. Hung, “One-Time password authentication protocol against theft attacks”, IEICE Trans. on Commun., vol.E89-B, no.12, pp. 3425-3427, 2006.
[11] W.C. Kuo, Y.C. Lee, “Attack and improvement on the one-time password authentication protocol against theft attacks”, Proc. of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, pp. 19-22, Aug. 2007.

Authors

Mijin Kim received her B.S., M.Ed. degrees from Sungkyunkwan University, Korea, in 1985, in 1989, respectively, and M.S. degree from Northeastern University, Boston, USA, in 1997. She is currently Ph.D. candidate in the School of Electrical and Computer Engineering of Sungkyunkwan University, Korea. Her research interests are cryptographic protocols, information security and network security.

Byunghee Lee received B.S. and M.S. degrees in computer engineering from Sungkyunkwan University, Korea, in 2005 and 2007, respectively. During 2005-2007, he worked in Information Security Group (ISG). He is currently Ph.D. course student of the School of Information and Communication Engineering. His interests are information security, reverse engineering, and information assurances.

Seungjoo Kim is a professor of School of Information and Communication Engineering of Sungkyunkwan University in Korea. His main research areas are cryptology and information security. He received his B.E., M.E., and Ph.D. degrees in Information Engineering from Sungkyunkwan University in 1994, 1996, and 1999 respectively. He joined KISA (Korea Information Security Agency) in December 1998 and remained until February 2004. In addition, since 2002, he has worked as an IT standard expert on behalf of Korea.

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University, Korea, in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently Professor of School of Information and Communication Engineering. His interests are on cryptology and information security. Especially, in the year 2002, he was occupied the president of KIISC (Korea Institute of Information Security & Cryptology).