논문 2011-6-38

동적 ID 기반 원격 사용자 인증 스킴의 보안성 개선

Improvements of a Dynamic ID-Based Remote User Authentication Scheme

주영도*, 안영화**

Young-Do Joo, Young-Hwa An

요 약 최근에 사용자 인증과정의 보안 취약점을 개선시킨 스마트 카드 기반의 사용자 인증 스킴들이 소개되었다. 2009년에 Wang[10]등은 Das[5]의 스킴의 보안 문제점을 개선하여 보다 효율적이고 안전성 있는 동적 ID 기반 원격사용자 스킴을 제안하였다. Wang 등은 자신들의 스킴이 인증과정에서 패스워드 독립성에 기인한 위협요인으로부터 안전할 뿐 아니라, 사용자와 원격 인증 서버 간 상호인증을 제공하고 있다고 주장한다. 본 논문은 Wang 등의 보안 스킴을 분석하고, 제안된 스킴이 중간자 공격 및 off-line 패스워드 추측 공격에 취약하다는 것을 증명한다. 또한 그들의 스킴이 상호인증을 제공하지 못함을 보여준다. 또한 본 논문에서는, 비록 스마트 카드의 비밀정보가 노출된다 하더라도, 이와같은 보안 문제점들을 해결한 개선된 스킴을 제안한다. 제안된 스킴은 사용자 위장 공격, 서버 위장 공격 그리고 off-line 패스워드 추측 공격에 안전하고, 계산 복잡도에서 Wang등의 스킴보다 효율적임을 알 수 있다.

Abstract Recently, many user authentication schemes using smart cards have been proposed to improve the security weaknesses in user authentication process. In 2009, Wang et al.[10] proposed a more effective and secure dynamic ID-based remote user authentication scheme to improve the security weakness of Das et al.'s scheme[5], and asserted that the improved scheme is secure against independent of password in authentication phase and provides mutual authentication between the user and the remote server. However, in this paper, we analyze the security of Wang et al. scheme and demonstrate that Wang et al.'s scheme is vulnerable to the man-in-the-middle attack and the off-line password guessing attack. In addition, we show that Wang et al. scheme also fails to provide mutual authentication. Accordingly, we propose an improved scheme to overcome these security weakness even if the secrete information stored in the smart card is revealed. Our proposed scheme can withstand the user impersonation attack, the server masquerading attack and off-line password guessing attack. Furthermore, this improved scheme provides the mutual authentication and is more effective than Wang et al.'s scheme in term of the computational complexities.

Key Words : Man-in-the-middle Attack, User Impersonation Attack, Server Masquerading Attack, Mutual Authentication

I. Introduction

With the rapid development of network technology, user authentication scheme in e-commerce and m-commerce has been becoming one of important security issues. However, lots of vulnerabilities have been exposed in the authentication scheme due to the careless password management and the sophisticated attack techniques. Several schemes and improvements for remote user authentication schemes using smart

*정회원, 강남대학교 컴퓨터미디어공학부
**정회원, 강남대학교 컴퓨터미디어공학부
접수일자 2011.11.17, 수정일자 2011.12.10
게재확정일자 2011.12.16

card have been proposed[1-10].

In 2004, Das et al.[5] proposed a dynamic ID-based remote user authentication scheme which has some merits, such as no verifier table, and user freedom to choose and change his password, etc. However, Awasthi et al.[6] in 2004 and Liao et al.[7] in 2005 showed that Das et al.' scheme is vulnerable to various attacks. In 2009, Wang et al.[10] proposed a more effective and secure dynamic ID-based remote user authentication scheme to overcome the security weakness of Das et al.'s scheme, and claimed that the improved scheme is secure against independent of password in authentication phase and provides mutual authentication to guarantee higher security.

In this article, we prove Wang et al.'s scheme to be weak to the man-in-the-middle attack and the off-line password guessing attack. In addition, our analysis on security flaws suggests that Wang et al.'s scheme also fails in offering mutual authentication. For the analysis of security weakness, we assume that an illegitimate attacker could obtain the values stored in the smart card by monitoring the power consumption, as pointed out in references[11-12]. To remedy Wang et al.'s security vulnerabilities, we propose an improved scheme while preserving all their merits, even if the secret information in the smart card is leaked.

The rest of this paper is organized as follows. In section II, we review Wang et al.'s scheme. In section III, we describe the security weekness of Wang et al.'s scheme. The proposed scheme is presented in section IV and its security analysis and performance evaluation are given in section V. Finally, brief conclusions are given in section VI.

II. Review of Wang et al.'s Scheme

In this section, we investigate Wang et al.'s scheme[10]. Wang et al.'s scheme based on hash function is divided into four phases: registration phase, login phase, authentication phase and password change phase. The registration phase is illustrated in Fig. 1. Also, the login phase and authentication phase are depicted in Fig. 2. The notations used throughout the scheme are follows:

- U_i: user i
- S: remote server
- PW_i: password of user i
- ID_i: identity of user i
- h(): one-way hash function
- ⊕: exclusive-OR operation

1. Registration Phase

This phase works whenever the user registers to the remote server.

1) The user submits his identifier ID_i to the server.
2) Upon receiving the ID_i, the server computes $N_i=h(PW_i)\oplus h(x)\oplus ID_i$, where x is a secrete of the server and PW_i is the password of U_i chosen by the server.
3) The server issues the information $\{N_i, y, h()\}$ to the smart card and sends it to the user through a secure channel, where y is the server's secret number stored in each registered user's smart card.

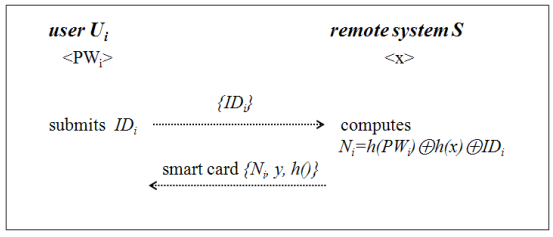

그림 1. 등록 단계
Fig. 1. Registration Phase of Wang et al.'s Scheme

2. Login Phase

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

1) The user inserts his smart card into a card reader and enters the identity ID_i and the password PW_i.
2) The smart card computes the dynamic identity of the user, $CID_i=h(PW_i)\oplus h(N_i\oplus y\oplus T)\oplus ID_i$, where

T is the current time.

3) The user sends the message $\{ID_i, CID_i, N_i, T\}$ to the server.

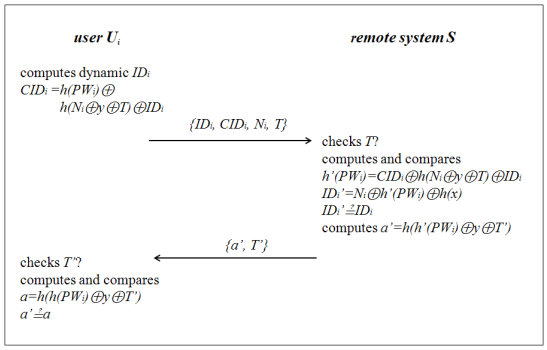

그림 2. 로그인 단계와 인증 단계
Fig. 2. Login Phase and Authentication Phase of Wang et al.'s Scheme

3. Authentication Phase

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

1) Upon the login request message $\{ID_i, CID_i, N_i, T\}$, the server checks the validity of the time interval between T and T′, where T′ is a time stamp when the server receives message. If it holds, the server accepts the login request of the user.
2) The server computes the equations such as $h'(PW_i)=CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i$ and $ID_i'=Ni \oplus h'(PW_i) \oplus h(x)$.
3) The server checks whether the computed value ID_i' equals to ID_i in the login request. If it holds, the user's login request is accepted.
4) The server computes $a'=h(h'(PW_i) \oplus y \oplus T')$ and then sends the message $\{a', T'\}$ to the user.
5) Upon receiving the reply message $\{a', T'\}$, the user checks the validity of the time interval between T^* and T′, where T^* is a time stamp when the user receives message.
6) If it holds, the user computes $a=h(h(PW_i) \oplus y \oplus T')$.
7) The user checks whether the received value a′ equals to the computed value a. If it holds, the user confirms that the server is valid.

4. Password Change Phase

This phase works whenever the user wants to change his password.

1) The user inserts his smart card into a card reader and enters the password PW_i, and request to change the password PW_i to new password PWnew.
2) The smart card computes $N_i^*=N_i \oplus h(PW_i) \oplus h(PWnew)$, and then replaces the N_i with the new N_i^*.

III. Security Weakness of Wang et al.'s Scheme

To analyze the security weaknesses, we assume that an attacker is one of legal users who was issued a smart card from the remote server and could obtain the values stored in his own smart card by monitoring the power consumption[11-12].

In this section, we will show that Wang et al.'s scheme is still vulnerable to the man-in-the-middle attack and the off-line password guessing attack, and that Wang et al.'s scheme cannot provide mutual authentication between the user and the server.

1. Man-in-the-middle Attack

A legal user U_i extracts N_i, and y from his smart card, and then he can easily derive h(x) by computing $h(x)=N_i \oplus h(PW_i) \oplus ID_i$. The attacker as the legal user U_i with a valid smart card can now perform the man-in-the-middle attack through the following steps. The processing of the man-in-the middle attack is illustrated in Fig. 3.

1) The attacker intercepts the login message $\{ID_j, CID_j, N_j, T_1\}$ of other user U_j, and then computes the following equations; $h(PW_j)=N_j \oplus h(x) \oplus ID_j$ and $CID_j^*=h(PW_j) \oplus h(N_j \oplus y \oplus T_1^*) \oplus ID_j$ where PW_j may be chosen at will by the attacker and T_1^* is the current time stamp.
2) The attacker sends the forged message

$\{ID_j, CID_j^*, N_j, T_1^*\}$ to the server.

3) Upon receiving the forged message, the server checks the validity of the time interval between T_1^* and T', where T' is a time stamp when the server receives message. If it holds, the server accepts the login request generated by the attacker.
4) The server computes the following equations: $h^*(PW_j)=CID_j^* \oplus h(N_j \oplus y \oplus T_1^*) \oplus ID_j$ and $ID_j^*=N_j^* \oplus h^*(PW_j) \oplus h(x)$.
5) Then the server authenticates the attacker as the legitimate user since $ID_j^*=ID_j$.
6) After the server computes $a^*=h(h(PW_j) \oplus y \oplus T_2)$, the server sends the reply message $\{a^*, T_2\}$ to the user.
7) The attacker intercepts the reply message $\{a^*, T_2\}$, and then computes $h(PW_j)=N_j \oplus h(x) \oplus ID_j$ and $a^{**}=h(h(PW_j) \oplus y \oplus T_2^*)$, where T_2^* is the current time stamp.
8) Then the attacker sends the forged reply message $\{a^{**}, T_2^*\}$ to the user U_j.
9) Upon receiving the forged reply message $\{a^{**}, T_2^*\}$, the user U_j checks the validity of the time interval between T_2^* and T'', where T'' is a time stamp when the user receives message. If it holds, the user accepts the forged reply message generated by the attacker.
10) The user computes $a=h(h(PW_j) \oplus y \oplus T_2^*)$, and then the user authenticates the attacker as the legitimate server since $a^{**}=a$.

In the above steps, the attacker can perform the man-in-the-middle attack without knowing the user's password if an attacker is one of legal users who have been issued a smart card from the remote server. Therefore, the attacker can impersonate as the legitimate user while talking to the server and masquerade as the legitimate server while talking to the user.

2. Password Guessing Attack

In this subsection, we will demonstrate that Wang et al.'s scheme is still vulnerable to the password guessing attack happening from two possible cases: (1) legal users with their smart cards and (2) illegal users with stolen smart cards.

■ With legal smart cards:

As described in earlier, a legal user U_i extracts N_i, and y from his smart card, and then he can easily derive h(x) by computing $h(x)=N_i \oplus h(PW_i) \oplus ID_i$. Now, the attacker as the legal user U_i with a valid smart card can perform off-line password guessing attack easily, in which each guess PW_j^* for PW_j can be verified by

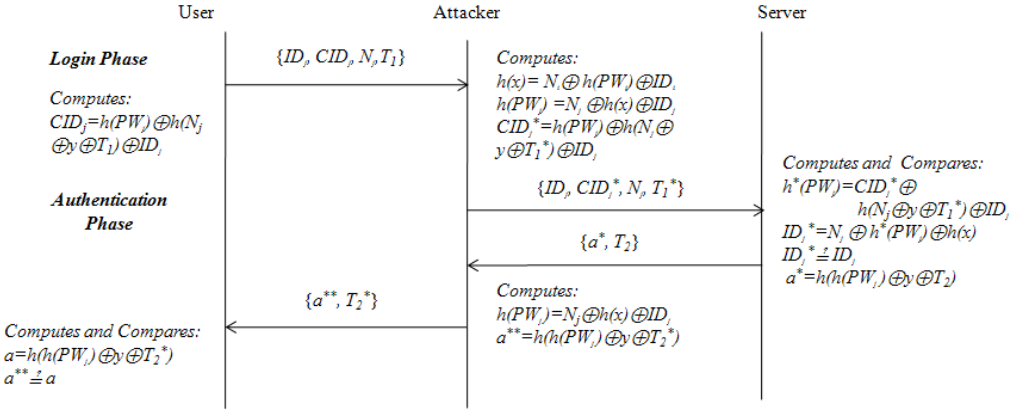

그림 3. 중간자 공격
Fig. 3. Man-in-the-middle Attack

the following steps.

1) From the login phase of other user U_j, the attacker computes $h(PW_j)=N_j \oplus h(x) \oplus ID_j$.
2) The attacker verifies the correctness of PW_j^* by checking $h(PW_j^*)=h(PW_j)$ repeatedly.
3) Finally, the attacker can find the correct password PW_j^*.

■ With stolen smart cards:

The attacker who has stolen the legal user's card extracts y from the stolen smart card by some means, and intercepts the user's login request message $\{ID_i, CID_i, N_i, T\}$ communicating between the user and the server. Now, the attacker with the stolen smart card can perform the off-line password guessing attack easily, in which each guess PW_i^* for PW_i can be verified by the following steps.

1) From the login phase of other user U_i, the attacker computes $h(PW_i)=CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i$.
2) The attacker verifies the correctness of PW_i^* by checking $h(PW_i^*)=h(PW_i)$ repeatedly.
3) Finally, the attacker can find the correct password PW_i^*.

3. Mutual Authentication

As you notice, Wang et al.'s scheme fails to provide the mutual authentication between the user and the remote server if any attacker with a smart card can obtain the values N_i, and y stored in his own smart card. Now, the attacker can easily derive h(x) by computing $h(x)=N_i \oplus h(PW_i) \oplus ID_i$ with the intercepted user's login request message $\{ID_j, CID_j, N_j, T\}$ communicating between the user and the server. Therefore, the attacker can impersonate the legal user easily with the forged login request message $\{ID_j, CID_j^*, N_j^*, T_1^*\}$ generated by computing the equations, $N_j^*=h(PW_j^*) \oplus h(x) \oplus ID_j$ and $CID_j^*=h(PW_j^*) \oplus h(N_j^* \oplus y \oplus T_1^*) \oplus ID_j$.

Also, after the attacker intercepts the reply message $\{a^*, T_2\}$ from the server, the attacker can compute $h(PW_j)=N_j \oplus h(x) \oplus ID_j$ and $a^{**}=h(h(PW_j) \oplus y \oplus T_2^*)$.

Accordingly, the attacker can masquerade the legal remote server easily by sending the forged reply message $\{a^{**}, T_2^*\}$.

IV. The Proposed Scheme

In this section, we propose the improved scheme based on the hash function which is divided into three phases: registration phase, login phase and authentication phase.

1. Registration Phase

This phase works whenever the user registers to the remote server. Fig. 4 shows the registration phase of the proposed scheme.

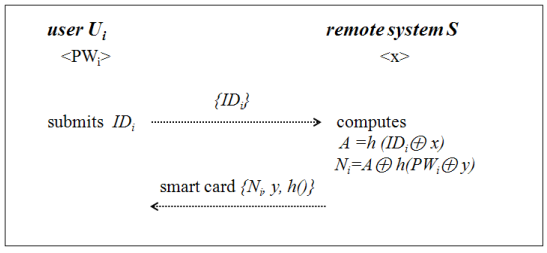

그림 4. 등록 단계
Fig. 4. Registration Phase of the Proposed Scheme

1) The user submits his identifier ID_i to the server.
2) The server computes $A=(h(ID_i \oplus x)$, $N_i=A \oplus h(PW_i \oplus y)$, where x is a secrete of the server and PW_i is the password of U_i chosen by the server. And y is the server's secret number stored in each registered user's smart card.
3) The server issues the information $\{N_i, y, h()\}$ to the smart card and sends it to the user through a secure channel.

2. Login Phase

This phase works whenever the user wants to login to the remote server. Fig. 5 depicts the login and authentication phase of the proposed scheme.

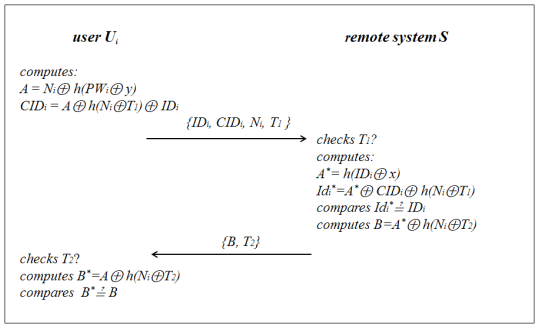

그림 5. 로그인 단계와 인증 단계
Fig. 5. Login Phase and Authentication Phase of the Proposed Scheme

1) The user inserts his smart card into a card reader and enters the identity ID_i and the password PW_i.
2) The smart card computes $A=N_i \oplus h(PW_i \oplus y)$, $CID_i=A \oplus h(N_i \oplus T_1) \oplus ID_i$, where T_1 is the current time.
3) The user sends the message $\{ID_i, CID_i, N_i, T_1\}$ to the server.

3. Authentication Phase

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

1) Upon the login request message $\{ID_i, CID_i, N_i, T_1\}$, the server checks the validity of the time interval between T_1 and T', where T' is a time stamp when the server receives message. If it holds, the server accepts the login request.
2) The server computes $A^*=h(ID_i \oplus x)$ and $ID_i^*=A^* \oplus CID_i \oplus h(N_i \oplus T_1)$.
3) The server checks whether the computed value ID_i^* equals to ID_i. If it holds, the user's login request is accepted.
4) The server computes $B=A^* \oplus h(N_i \oplus T_2)$ and then sends the message $\{B, T_2\}$ to the user.
5) Upon receiving the reply message $\{B, T_2\}$, the user checks the validity of the time interval between T_2 and T'' where T'' is a time stamp when the user receives message.
6) If it holds, the smart card computes $B^*=A \oplus h(N_i \oplus T_2)$
7) The smart card checks whether the received value B equals to the computed value B^*. If it holds, the user confirms that the server is valid.

V. Security Analysis and Performance Evaluation of the Proposed Scheme

1. Security Analysis

To analyze the security of the proposed scheme, we assume that an attacker can access a user's smart card and extract the values stored in the smart card by some means[11-12], and intercepts the messages communicating between the user and the server. Here, we only discuss the user impersonation attack, the server masquerading attack, the password guessing attack, and the mutual authentication.

■ User Impersonation Attack

To impersonate as the legal user, an attacker attempts to make the forged login request massage which can be authenticated to the server. However, the attacker cannot impersonate as the user by forging the login request massage, because the attacker does not compute the forged login message CID_i^* and N_i^* without knowing the remote server's secret value x.

■ 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 B^* without knowing the remote server's secret value x.

■ Password Guessing Attack

To perform the password guessing attack, the attacker attempts to extract the secret values from the user's smart card. Then the attacker attempts to derive the user's password PW_i from the equation $N_i=A \oplus$

$h(PW_i \oplus y)$ in the registration phase. However, the attacker cannot guess the user's password PW_i, because the attacker does not know the server's secret value x.

■ Mutual Authentication

As described in the user impersonation attack and the server masquerading attack, the proposed scheme provides the mutual authentication between the user and the remote server. The attacker cannot succeed in devising the forged messages each phase without knowing the remote server's secret value x, even if the attacker can extract the secret information in the user's smart card.

The security comparison of Wang et al.'s scheme and our proposed scheme is summarized in Table 1. In contrast to Wang et al.'s scheme, the proposed scheme is relatively more secure.

표 1. 안전성 비교분석
Table 1. Security Comparison

Security Properties	Wang et al.'s Scheme	Proposed Scheme
User Impersonation Attack	possible	impossible
Server Masquerading Attack	possible	impossible
Password Guessing Attack	possible	impossible
Mutual Authentication	not supported	supported

2. Performance Evaluation

In this section, we evaluate the efficiency of the proposed scheme in terms of the computational complexities. As you notice from Table 2, the proposed scheme is slightly more effective than Wang et al.'s scheme in that our scheme requires only 4 THs and 8 TXs during the authentication phase, including the mutual authentication.

표 2. 성능 비교 평가
Table 2. Comparison of Computational Complexities

Phase	Wang et al.'s Scheme	Proposed Scheme
Registration	1TH+2TX	2TH+3TX
Login	2TH+4TX	2TH+5TX
Authentication	5TH+10TX	4TH+8TX

<TH: time for performing a one-way hash function>
<TX: time for performing an exclusive-OR operation>

VI. Conclusions

In 2009, Wang et al. proposed a more effective and secure dynamic ID-based remote user authentication scheme to improve the security weakness of Das et al.'s scheme. They asserted that their scheme offer better security against independent of password in authentication phase and the mutual authentication. However, we demonstrated that Wang et al.'s scheme is not secure against the man-in-the-middle attack and the off-line password guessing attack. In addition, Wang et al.'s scheme turns out to be infeasible for offering mutual authentication.

Accordingly, we proposed the improved scheme to overcome these security weakness and withstand the user impersonation attack and the server masquerading attack etc. We proved that the proposed scheme is more secure and efficient than Wang et. al's scheme through the comparison of the security properties and performance evaluation by the computational complexities.

References

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

[2] M. S. Hwang, and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics, Vol. 46, pp. 28-30, 2000.

[3] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security Enhancement for the timestamp-based password Authentication Scheme Using Smart Cards", Computers and Security, 22(7), pp. 591-595, 2003.

[4] 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.

[5] 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.

[6] A. K. Awasthi, and S. Lal, "Security Analysis of a Dynamic ID based Remote User Authentication Scheme ", http://eprint.iacr.org/2004/238.pdf.

[7] I. E. Liao, C. C. Lee, and M. S. Hwang, "Security Enhancement for a Dynamic ID based Remote User Authentication Scheme", in IEEE CSPress, NWeSP'05, pp. 437-440, 2005.

[8] 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.

[9] 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.

[10] Y. Y. Wang, J. Y. Liu, and F. X. Dan, "A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme", Computer Communications, Vol. 32, pp. 583-585, 2009.

[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.

저자 소개

주 영 도(정회원)

- 한양대학교 전자통신공학과 학사
- 미국 University of South Florida 컴퓨터공학과 석사
- 미국 Florida State University 전산학과 박사
- KT 통신망 연구소 선임연구원
- 시스코 시스템즈 코리아 상무
- 화웨이 기술 코리아 부사장
- 현 강남대학교 컴퓨터미디어공학부 교수

<주관심분야 : 정보보안, 네트워크 보안, 정보검색>

안 영 화(정회원)

- 성균관대학교 전자공학과 박사
- 해군사관학교 전자공학과 교수
- 강남대학교 학술정보처장
- 강남대학교 전산정보원장
- 미국 Florida State University 방문 교수
- 현 강남대학교 컴퓨터미디어공학부 교수

<주관심분야 : 시스템 보안, 네트워크 보안, 정보보안>