www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.2.081

# 사용자 익명성을 보장하는 안전하고 개선된 원격 사용자 인증스킴

## A Robust and Secure Remote User Authentication Scheme Preserving User Anonymity

신광철(Kwang-Cheul Shin)*

**초 록**

원격사용자 인증스킴은 안전하지 않은 통신상에서 원격 서버에게 사용자의 적법함을 확인하는 방법이다. 현재, 스마트카드 기반의 원격사용자 인증스킴들은 상호인증을 위해 연산비용은 낮추면서 간편한 기법이 넓게 적용되어오고 있다. 2009년, Wang et al.'s는 스마트카드를 이용한 동적 ID기반의 원격사용자 인증스킴을 제안했다. Wang et al.'s 스킴은 여러 가지 공격에 안전하고 서버에서 선택된 강력한 패스워드에 의해 익명성이 보장된다고 주장했다.

그러나 본 논문에서는 Wang et al.'s 스킴이 인증과정에서 사용자의 익명성을 제공하지 않는 취약점이 있다고 지적한다. 또 사용자에게 패스워드 선택의 권한이 없으며 제한된 replay 공격에 취약하다. 특히 사용자에게 전송된 파라미터 y는 매우 부적절하게 사용되고 있다. 이러한 보안의 결점을 극복하기 위해 Wang et al.'s 스킴의 식별된 약점을 보완하고 사용자와 원격서버 간에 완전한 익명성보장과 향상된 인증스킴을 제안한다.

**ABSTRACT**

Remote user authentication is a method, in which remote server verifies the legitimacy of a user over an common communication channel. Currently, smart card based remote user authentication schemes have been widely adopted due to their low computational cost and convenient portability for the mutual authentication. 2009 years, Wang et al.'s proposed a dynamic ID-based remote user authentication schemes using smart cards. They presented that their scheme preserves anonymity of user, has the feature of storing password chosen by the server, and protected from several attacks. However, in this paper, I point out that Wang et al.'s scheme has practical vulnerability. I found that their scheme does not provide anonymity of a user during authentication. In addition, the user does not have the right to choose a password. And his scheme is vulnerable to limited replay attacks. In particular, the parameter y to be delivered to the user is ambiguous. To overcome these security faults, I propose an enhanced authentication scheme, which covers all the identified weakness of Wang et al.'s scheme and an efficient user authentication scheme that preserve perfect anonymity to both the outsider and remote server.

**키워드** : 인증, 익명성, 스마트카드, 위장공격
Authentication, Anonymity, Smart Card, Forgery Attack

---

In this paper was conducted by grant of Sungkyul University academic study support, 2013 year.
* Corresponding Author, Professor in Dept. of Industrial Management Engineering, Sungkyul University (skcskc12@sungkyul.edu)
2013년 02월 28일 접수, 2013년 04월 08일 심사완료 후 2013년 04월 22일 게재확정.

# 1. Introduction

Development of information communication technology coming to activity of internet banking and electronic business, and smart card of medium is generalized prevailing for user authentication of electronic signature certificate management center with cyber cash, traffic card. Smart card authentication schemes have been widely deployed to verify the legitimacy of remote user's login request. Also, smart card is due to their low computation cost and convenient for the authentication purpose [1, 3, 5, 8~10, 12, 19~20]. In initial password authentication schemes, the server has to store a password table to save passwords of all the registered users of the system [8]. Afterwards, Hwang and Li pointed out that when the password table was stolen or modified in this scheme, the whole authentication scheme will be influence. And they proposed a remote user authentication scheme without using the password table [5]. A common feature among most of the presented schemes is that the user's identity is static in all the login and authentication phase, which may leak some information about that user and can create vulnerability of id theft and location tracking during the message transmission over an common channel [14~17]. To overcome this vulnerability, Das et al.'s [2] proposed a dynamic ID-based remote user authentication scheme. But 2009 years, Wang et al.'s [18] showed that Das et al.'s scheme is completely insecure for its independence of using passwords, does not provide mutual authentication, and cannot resist forge server attack. Wang et al.'s proposed a dynamic ID-based remote user authentication scheme and Wang et al.'s scheme claimed that a secure and efficient than the DAS scheme. In 2011, Khan et al.'s [6] proposed an enhanced authentication scheme which covers all the identified weaknesses of Wang et al.'s scheme and is more secure and efficient for practical application environment. In this paper, I showed that Wang et al.'s scheme is susceptible to forgery (impersonation) attack and insider attack. In addition, their scheme cannot ensure the user's anonymity and has vulnerability to a limited replay attack. Especially, parameter (random number y) of server is the remote server's secrete number stored in each registered user's smart card that is not description using of parameter y in server's authentication phase. To overcome the security vulnerability of Wang et al.'s scheme, I propose an efficient user authentication scheme using secret key to generation of cipher text that preserve perfect anonymity to both the outsider and remote server. Rest of the paper is organized as follow: Section 2 briefly reviews Wang et al.'s scheme, Section 3 evaluate on the weaknesses and security vulnerability of their scheme, Section 4 presents my proposed robust scheme, Section 5 discusses the security analysis of my scheme, Section 6 provides security features of the presented scheme, and at the end, Section 7 concludes this paper.

## 2. Review of Wang et al.'s Scheme

In this section, I briefly review Wang et al.'s scheme which consists of four parts namely, registration phase, login phase, verification phase and password change phase. The scheme is illustrated in <Figure 1> And the notations used in this scheme are shown in <Table 1>.

### 2.1 Registration Phase

The user U sends the registration request to the remote server S:

〈Table 1〉 Notations

| Symbol | Description |
|---|---|
| U | The user |
| pw | The password of U |
| ID | The identity of U |
| S | The remote server |
| h(.) | A one-way hash function |
| ⊕ | Bitwise XOR operation |
| ⇒ | A secure channel |
| → | A common channel |

(ⅰ) U submits ID to S.

(ⅱ) S compute Ni = h(pw) ⊕ h(x) ⊕ ID, where x is secrete of the remote server, pw is the password of U chosen by S.

(ⅲ) S personalizes the smart card with the parameters [h(.), Ni, y], where y is the remote server's secrete number stored in each registered user's smart card.

(ⅳ) S⇒U : pw and smart card.

### 2.2 Login Phase

When U wants to login into S, he inserts smart card in the terminal and keys in his identity ID and password pw, then the smart card performs the following steps:

(ⅰ) Computes dynamic ID: CIDi = h(pw) ⊕ h(Ni ⊕ y ⊕ T) ⊕ ID, T is the current date and time.

(ⅱ) U→S : ID, CIDi, Ni, T.

### 2.3 Verification Phase

When the remote server S receives the login request [ID, CIDi, Ni, T] at time T', S verifies as:

(ⅰ) Checks the validity of time stamp with the current data and time T', If (T'-T) ≤△T holds, S accepts the login request of U, otherwise the login request is rejected.

(ⅱ) Computes h'(pw) = CIDi ⊕ h(Ni ⊕ y ⊕ T) ⊕ ID.

(ⅲ) Computes ID = h'(pw) ⊕ h(x) ⊕ Ni and verifies whether it is equal to ID or not. If it holds, the remote server S accepts the login request, otherwise login request is rejected. Then S computes a' = h(h(pw) ⊕ y ⊕ T') using the result of step (ⅱ).

| User | | Server |
|---|---|---|
| | **[Registration]** | |
| Selected ID | -------- ID ---------> | selected U's password pw<br>compute Ni = h(pw) ⊕ h(x) ⊕ ID<br>selected U's secret number y |
| | <--- pw and smart card --- | smart card stored [h(.), Ni, y] |
| | **[Login and Authentication]** | |
| Input ID, pw<br>compute CIDi = h(pw) ⊕ h(Ni ⊕ y ⊕ T) ⊕ ID | | |
| | -- ID, CIDi, Ni, T ----> | verification T<br>h'(pw) = CIDi ⊕ h(Ni ⊕ y ⊕ T) ⊕ ID<br>compute ID = h'(pw) ⊕ h(x) ⊕ Ni<br>check ID |
| | <-------- a', T' ------ | compute a' = h(h(pw) ⊕ y⊕T') |
| verification T<br>compute a" = h(h(pw) ⊕ y ⊕ T')<br>compares a' = ?a" | | |
| | **[Password change]** | |
| computes $N^*i$ = Ni ⊕ h(pw) ⊕ h($pw_{new}$) | | |

〈Figure 1〉 Wang et al.'s Scheme

(iv) S→U : [a', T']
Upon receiving the replay message [a', T'] at time T", U verifies as:

(v) U check whether T"-T ≥ △T, if not U computes a" = h(h(pw) ⊕ y ⊕ T'), and compares it with the received a', if it holds, U confirms that S is valid.

## 2.4 Password Change Phase

When U wants to change his password, he inserts smart card into the terminal device, keys in the password pw, and requests to change the password to new one, i.e. $pw_{new}$. Then, the smart card computes $N^*i$ = Ni ⊕ h(pw) ⊕ h($pw_{new}$) and replaces Ni the with the new $N^*i$ in the smart card.

# 3. Security Analysis of Wang et al.'s Scheme

## 3.1 Stolen Attack

When the smart card is lost or stolen, unauthorized users can easily guess the password of the user by using password guessing attack, or can impersonate the user to login to the system. Messerges et al.'s [13] pointed out that all existing smart cards can not prevent the information stored in them from being extracted by techniques such as monitoring their power consumption. The h(), Ni and y are embedded in the user's smart card. An adversary (third-party) can analyze by sniffing the login request messages (ID, CIDi, Ni,

T) with use of the data embedded in the smart card.

### 3.2 Contradiction of Parameter y

At registration phase (iii), a parameter y has been generated and stored in smart card. The parameter y is a random number, generated by the remote server. Therefore the value of y is different for each user. Here what we are talking about is that the parameter y is not stored in any server. In registration phase, server S personalizes the smart card with the parameters [h(), Ni, y], where y is the remote server's secrete number stored in each registered user's smart card. In login phase, user sending ID, CIDi, Ni, T to server. And the server compute h'(pw) = CIDi $\oplus$ h (Ni $\oplus$ y $\oplus$ T) $\oplus$ ID at the verification phase 2.3 (ii). Even though the user does not forward y to the server, the server compute h'(pw). Hence, this is a contradiction.

### 3.3 Forgery(impersonation) Attack

Assume that stolen attack is successful. The h'(pw) can be extracted with use of the data (h(), Ni, y) stored in smart card and the data sniffed from login request message (ID, CIDi, Ni, T). Subsequently, the adversary compute the perfect value of CIDi using arbitrary time T and generates login request message disguising as a legitimate user. The server S can successfully pass the processes of (i), (ii) and (iii) at 2.3 verification phase.

### 3.4 Non Anonymity

Wang et al.'s scheme does not preserve the anonymity of U, In the verification phase, ID and CIDi are transmitted to the authentication server S over insecure channel in the login message m = [ID, CIDi, Ni, T]. In some authentication scenarios, e.g. electronic banking or electronic payment system, it is very important to preserve the privacy of a user because an adversary sniffing the communication channel can eavesdrop the communication parties involve in the authentication process and can easily analyze the transaction being performed by U [11]. Thus, In Wang et al.'s scheme fails in providing the privacy and anonymity of U during the authentication phase [6].

### 3.5 Limited Replay Attack

Wang et al.'s scheme utilizes time stamp T in order to defend the re-transmission attack. Time stamp T is verified at 2.3 verification phase (i). A time stamp based protocol generally maintains a tolerant window $\triangle$T to allow a reasonable time difference between transmission time T and receive time T'. The adversary can be allowed to send an identical message repeatedly within a short period less than $\triangle$T. All the messages transmitted within time T, where (T'-T) $\leq \triangle$T is true, can suc-

cessfully pass the process of 2.3 verification phase (i). Therefore, the re-transmission attack is successfully possible at any time in the protocol using time stamp only if the attack is attempted within limited times [4].

# 4. The Improved Scheme

Improvement ideas:

- User's arbitrary selection of password and defense against insider attack.
- Ensure the anonymity with use of secret key
- Defense against replay attack
- Defense against impersonate and stolen attack
- Contradiction of parameter y

The improved scheme is also divided into three phase: registration, login, authentication, and password change phases.

## 4.1 Registration Phase

The additional notation used in the proposed scheme is as follows:

〈Table 2〉 Additional Notations

| Symbol | Description |
|---|---|
| Ui | The user i |
| pwi | The password of Ui |
| IDi | The identity of Ui |

The user Ui sends the registration request to the remote server S:

(ⅰ) Ui chooses a password pwi and compute h(pwi ⊕ IDi). He submits IDi and h(pwi ⊕ IDi) to S through a secure channel.

(ⅱ) S then chooses a secret number yi, computes Ni = h(IDi ⊕ h(x)) ⊕ h(IDi ⊕ pwi) ⊕ h(yi) and I = h(IDi ⊕ x) ⊕ h(x), where x is the secret key of S.

(ⅲ) S personalizes the smart card with the parameters [IDi, h(), Ni, I] and where yi is the secret code of remote server. S returns smart card to the registered user and yi.

(ⅳ) S ⇒ Ui : yi and smart card.

## 4.2 Login Phase

When a user wants to login the remote server, He inserts the smart card to the terminal and keys the password pwi and yi, then the smart card will perform the following steps.

(ⅰ) Password check:
P = h(pwi ⊕ IDi) ⊕ Ni.
Ni = ?P ⊕ h(pwi ⊕ IDi), accept or reject.

(ⅱ) Compute dynamic ID : CIDi = h(IDi ⊕ pwi) ⊕ h(Ni ⊕ h(yi) ⊕ T) where T is the current date and time.

(ⅲ) The user generates a random number ri.

(ⅳ) Compute : M = Ni ⊕ h(IDi ⊕ pwi) ⊕ ri.

(ⅴ) Compute : K = I ⊕ h(yi) ⊕ ri.

| User | Server |
|---|---|
| **[Registration]** | |
| Selected IDi, pwi --- IDi, h(pwi ⊕ IDi) ---> | selected U's secret number yi<br>compute Ni = h(IDi ⊕ h(x)) ⊕ h(IDi ⊕ pwi) ⊕ h(yi)<br>I = h(IDi ⊕ h(x)) ⊕ h(x) |
| <--- yi and smart card --- | smart card stored [IDi, h(.), Ni, I] |
| **[Login and Authentication]** | |
| Input yi, pwi<br>P = h(pwi ⊕ IDi) ⊕ Ni.<br>Ni = ?P ⊕ h(pwi ⊕ IDi)<br>CIDi = h(IDi ⊕ pwi) ⊕ h(Ni ⊕ h(yi) ⊕ T)<br>input random number ri<br>M = Ni ⊕ h(IDi ⊕ pwi) ⊕ ri<br>K = I ⊕ h(yi) ⊕ ri -- M, $E_K$[CIDi, T, h(y), Ni]--> | K = M ⊕ h(x)<br>$D_K$ [CIDi, T, h(yi), Ni]<br>verification T<br>h(IDi ⊕ pwi) = Ni ⊕ h(IDi ⊕ h(x)) ⊕ h(yi)<br>$CIDi^*$ = ?h(IDi ⊕ pwi) ⊕ h(Ni ⊕ h(yi) ⊕ T) |
| <------ $E_K$[D, $T^*$] ------- | D = h($T^*$ ⊕ T ⊕ CIDi ⊕ h(IDi ⊕ pwi)) |
| verification $T^*$<br>$D^*$ = h($T^*$ ⊕ T ⊕ CIDi ⊕ h(IDi ⊕ pwi))<br>check D = ?$D^*$ | |
| **[Password change]** | |
| compute $Ni_{new}$ = Ni ⊕ h(IDi ⊕ pwi) ⊕ (IDi ⊕ $pw_{new}$) | |

〈Figure 2〉 Propose Scheme

(vi) Ui → S: [M, $E_K$ [CIDi, T, h(yi), Ni], the $E_K$ [CIDi, T, h(yi), Ni] is ciphertext of encrypted using secret key K.

## 4.3 Authentication Phase

When the remote server S receives the log-in request

[M, $E_K$ [CIDi, T, h(yi), Ni] at time T', server authenticates the user Ui as follows:

(i) Compute K with server's secret key x, K = M⊕h(x) then decrypt the message $D_K$ [CIDi, T, h(yi), Ni].

(ii) S verifies if (T'-T) ≤ △T. If it holds, S accepts Ui the login request, where △T is an expected valid time interval. And then S compute h(IDi ⊕ pwi) = Ni ⊕ h(IDi ⊕ h(x)) ⊕ h(yi) and check if $CIDi^*$ = h(IDi ⊕ pwi) ⊕ h(Ni ⊕ h(yi) ⊕ T). If it holds, S accepts Ui to login the system. Otherwise, reject it.

(iii) Then S compute D = h($T^*$ ⊕ T ⊕ CIDi ⊕ h(IDi ⊕ pwi)), where $T^*$ is the current data and time of S.

(iv) S → Ui : $E_K$ [D, $T^*$], the $E_K$[D, $T^*$] is ciphertext of encrypted using the secret key K.

(v) After receiving the replay message at

the time T", Ui decrypts the message $D_K$ [D, $T^*$] using the secret key K.

(vi) Ui verifies if whether $(T"-T^*) \leq \triangle T$. If it holds, Ui compute $D^* = h(T^* \oplus T \oplus CIDi \oplus h(IDi \oplus pwi))$, and verifies if D = ?$D^*$, If it holds, Ui confirms that the communicates with valid S.

### 4.4 Password Change Phase

Ui inserts his smart card to the card reader of a terminal, and inputs pwi and his new password $pw_{new}$. Smart card compute

$$Ni_{new} = Ni \oplus h(IDi \oplus pwi) \oplus (IDi \oplus pw_{new}) = h(IDi \oplus h(x)) \oplus h(IDi \oplus pw_{new}) \oplus h(yi)$$

## 5. Security Analysis of the Improved Scheme

In this section, I am going to demonstrate that my scheme is secure:

### 5.1 User Anonymity

user Ui anonymity is preserved at each login request. Ui compute to protect the user's anonymity and security of message, messages are transmitted after being encrypted using security information, K (K = I $\oplus$ h(yi)). The $E_K$ [CIDi, T, h(yi), Ni] is ciphertext of encrypted using secret key K. If the third party intends to know K, he/she needs to generate M. In order to generate M, he/she needs to know the user's password. However, the password cannot be revealed because it has been generated by being hashed after XOR with ID. However, the server S can decrypt the message after generating secret key K by using its own secret key x. Compute K with server's secret key x, K = M $\oplus$ h(x) then decrypt the message $D_K$ [CIDi, T, h(yi), Ni]. Hence, in the presented scheme, an adversary cannot identify the person trying to login into the server.

### 5.2 Smart Card Loss Attack

When the smart card is lost or stolen, unauthorized users can easily change the password of the smart card, or can guess the password of the user by using password guessing attack, or can impersonate the user to login to the system. To make sure the user provides the correct password at the login phase, the verifying process needs to be performed with the user's password through computing (Ni = ?P $\oplus$ h(pwi $\oplus$ IDi)). In the situation where the smart card is lost, the unauthorized user could probably obtain the password by guessing it. To make the probability zero, password verification should be conducted at the login phase.

### 5.3 Solution of Parameter yi

The yi provided by server to each user is generated to be a hash value by invoking hash

function. Prior to sending the login request message to the server, it is encrypted using secrete key. And then the server uses h (yi) for deriving h (pwi ⊕ IDi) and CIDi.

### 5.4 Securely Chosen and Update Password

In the proposed scheme, the legitimate smart card holder can freely choose and change his password without any regardless of contacting the remote server S. Also, any other person, even having stolen or lost smart card can not using the smart card according 4.2 Login phase because third-party (adversary) cannot know pwi and yi of the Ui.

### 5.5 Replay Attack

The replay attacks cannot performance in the proposed scheme. That is, replaying neither the login message [M, $E_K$ [CIDi, T, h(y), Ni] of login phase nor response message $E_K$ [D, $T^*$] of authentication phase will not succeed since the encrypted message. Since the attack is possible during the period of tolerant window $\triangle T$ in the time stamp based method, the proposed protocol applies the encryption scheme with session secrete key k.

### 5.6 Forge(Impersonate) Attack

If user Uj wants to impersonate Ui to login the remote server, he should know h(pwi ⊕ IDi). Uj knows Ni, h(yi), I. but he cannot obtain h(pwi ⊕ IDi) from Ni ⊕ h(IDi ⊕ h(x)) ⊕ h(yi), because he cannot know pwi of the Ui. On the other hand, each user's yi is different, and it does not store the smart card, he cannot use his Nj to compute h(pwi ⊕ IDi). That is, the proposed scheme can resist the impersonate attack. Of cause, it can resist the forgery attack. Therefore, any other person, even having stolen or lost smart card can not using the smart card according 4.2 Login phase because third-party cannot know pwi and yi, random number ri of the Ui.

### 5.7 Stolen Attack

The improved scheme can resist the stolen attack. If the user lost his smart card, the improved scheme still secures. Let's assume that smart card is stolen, or theft. The third party may know the value(Ni, I) of the smart card. However, in order to compute the CIDi, the third party should be aware pwi and yi of user. Also, the third party server's secret key x is unknown. Therefore, the contents of M is unknown.

## 6. Security Feature Analysis of the Proposed Scheme

In this section, the proposed scheme summarize the security features of scheme and compare its security and with Wang et al.'s

〈Table 3〉 Security Comparison of the Proposed Scheme with Wang et al.'s Scheme

| Security features | Das et al.'s [2] | Wang et al.'s [18] | | The proposed scheme | |
|---|---|---|---|---|---|
| User anonymity | safety | vulnerable | User anonymity is not preserved at each login request | safety | Login message is cipher-text of encrypted using secret key k. |
| Privilege user-selectable password | vulnerable | vulnerable | The password is chosen by the remote server S without the consent of user | safety | User has choice of choosing his own password, until change user password. |
| Replay attack | weak | weak | The adversary can be allowed to send an identical message repeatedly within a short period less than $\triangle T$ | safety | Login message and response message of authentication phase is not succeed since the encrypted message. |
| forgery (Impersonate) attack | weak | weak | The h'(pw) can be extracted with use of the data (h(), Ni, y) stored in smart card [6]. | safety | Each user's yi does not store the smart card. So, adversary cannot compute h(pwi $\oplus$ IDi). |
| Insider attack | weak | weak | Vulnerability to online banking, e-mail has been selected by the user's password on the server. | safety | User has choice of choosing his own password, until change user password. At least, it is safer than the wang et al.'s scheme. |
| Parameter y | not applicable | contradiction | The user does not forward parameter y to the server, But the server compute h'(pw). | non-contradiction | Parameter y sending the login request message to the server, it is encrypted using secrete key. |
| Smart card loss attack | weak | weak | When the user's smart card is stolen or theft, the adversary can find out the contents of the Ni, y. Also, transfer information [IDi, T, CIDi, Ni] can be elicited to value of CIDi. | safety | Let's assume that smart card is stolen, or theft. The third party may know the value (Ni, I) of the smart card. However, in order to compute the CIDi, the third party should be aware pwi and yi of user. |
| Use of cipher key | not use | | | use | |

scheme. <Table 3> demonstrates that the proposed scheme is more secure and robust than Wang et al.'s scheme and achieves more security features. The proposed scheme not only does not maintain any verifier table, but also enhances the security. The reason that there is no secret numbers in the smart card, it is a random number ri and the parameters yi provided by the server. it can withstand replay attack, impersonate and forgery attack, it also guarantees user anonymity. The proposed scheme, using a symmetric key cipher for the anonymity and security. The symmetric key cryptography largely on the speed of the operation is not affected.

## 7. Conclusion

The remote user's smart card authentication is required for the protection of privacy, anonymity and prevent the location tracking.

In this paper, I have presented cryptanalysis and weakness of Wang et al.'s dynamic ID-based remote user authentication scheme. And I showed that Wang et al.'s scheme is vulnerable to impersonation attack and limited replay attack, does not preserved anonymity of a user. Also it was also pointed out the contradictions of the parameter y. To overcome the identified problems, I have proposed a more completely and secure remote user authentication scheme preserving user anonymity. which improves all the identified weakness of Wang et al.'s scheme and is more secure. For this purpose, a symmetric key cryptography was used. This paper shows that the proposed technique is more secure than Wang et al.'s scheme by presenting the results of the comparative analysis between the two schemes in terms of security. It is expected that the scheme proposed in this thesis can be used in various applications for which smart cards are used.

## References

[1] Chen, C. M. and Ku, W. C., "Stolen-verifier attack on two new strong-password authentication protocol," IEICE Transactions on communications, E85-B, pp. 2519-2521, 2002.

[2] Das, M. L., Saxena, A., and Gulati, V. P., "A dynamic ID-based remote user authentication Scheme," IEEE Transactions on Consume Electronics, Vol. 50, No. 2, pp. 629-631, 2004.

[3] Fan, C. I., Chan, Y. C., Zhang, Z. K., "Robust remote authentication scheme with smart cards," Computers and Security, Vol. 24, No. 8, pp. 619-628, 2005.

[4] Gong, L., "A security risk of depending on synchronized clock," Operating System Review, Vol. 26, No. 1, pp. 49-53, 1992.

[5] Hwang, M. S. and Li, L. H., "A new ernote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, 2000.

[6] Khan, M. K., Kim, S. K., and Alghathbar, K., "Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, Vol. 34, No. 3, pp. 305-309, 2011.

[7] Ku, W. C. and Chen, S. M., "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart card," IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 204-207, 2004.

[8] Lamport, L., "Password authentication with insecure communication," Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[9] Lee, C. C., Hwang, M. S., and Yang, W. P., "A Flexible Remote User Authentication Scheme using Smart Cards," ACM Operat-

ing System Review, Vol. 36, No. 4, pp. 23-29, 2002.

[10] Lee, N. Y. and Chiu, Y. C., "Improved remote authentication scheme with smart card," Computer Standard and Interface, Vol. 27, No. 2, pp. 177-180, 2005.

[11] Liao, I. E., Lee, C. C., and Hwang, M. S., "Security enhancement for a dynamic ID-based remote user authentication scheme," KOREA : International Conference on Next Generation Web Services Practices, IEEE, 2005.

[12] Liao, Y. P. and Wang, S. S., "A secure dynamic ID-based remote user authentication scheme for multi-server environment," Computer Standards and Interfaces, Vol. 31, No. 1, pp. 24-29, 2009.

[13] Messerges, T. S., Dabbish, E. A., and Sloan, R. H., "Examining Smart Card Security under the Threat of Power Analysis Attack," IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, 2002.

[14] Shin, K. C., "Vulnerability Analysis and Improvement in Man-in-the-Middle Attack for Remote User Authentication Scheme of Shieh and Wang et al.'s using Smart Card," The Journal of Society for e-Business Studies, Vol. 17, No. 4, pp. 1-16, 2012, (dx.doi.org/10.7838 /jsebs.2012.17.4.001).

[15] Shin, K. C., "Analysis and Countermeasure for Authentication Scheme of Qi Xie's Based on Variable Authenticator," The Korean Institute of Information Technology, Vol. 10, No. 1, pp. 139-146, 2012.

[16] Shin, K. C., "Vulnerability Analysis and Improvement of a Remote User Authentication Scheme by Legitimate Members," Korea Knowledge Information Technology Sciety, Vol. 7, No. 6, pp. 181-192, 2012.

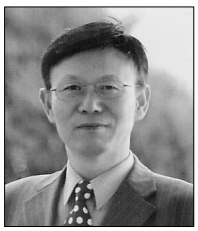
[17] Song, R., "Advance smart card based password authentication protocol," Computer Standards and Interface, Vol. 32, No. 5-6, pp. 321-325, 2010.

[18] Wang, Y. Y., Kiu, J. Y., Xiao, F. X., and dan, J., "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, Vol. 32, No. 4, pp. 583-585, 2009.

[19] Xie, Q., Wang, J. K., Chen, D. R., and Wang, X. Y., "A novel user authentication scheme using smart card," College of Computer Science. Zhejiang University, Hangzhou, 310027, P R China, and Graduate School. Hangzhou Normal University, 2008.

[20] Xu, J., Zhu, W., and Feng, D., "An improved smart card based password authentication scheme provable security," Computer Standard and Interface, Vol. 31, No. 4, pp. 723-728, 2009.

## 저 자 소 개




| | |
|---|---|
| Shin Kwang-Cheul | (E-mail : skcskc12@hanmail.net) |
| 1985 | Seoul National University of Science and Technology Computer Science |
| 1990 | Korea National Defense University Computer Science |
| 2003 | Sungkyunkwan University Dept. Information Engineering |
| 2004~Current | Sungkyul University, Division of Industrial Management Engineering |
| Interest Field | Smart card security, E-Payment System, Network and RFID security |