한국산학기술학회논문지
Vol. 10, No. 2, pp. 327-333, 2009

Cryptanalysis of Remote User Authentication Scheme

Jong-Seok Choi[1], Seung-Soo Shin[1*] and Kun-Hee Han[2]

원격 사용자 인증 구조의 암호학적 분석

최종석[1], 신승수[1*], 한군희[2]

Abstract In 2004, Das et al. proposed a scheme for preserving a user anonymity. However, In 2005, Chien and Chen pointed out that Das et al. scheme fail to protect the user anonymity, and proposed a new scheme. And then in 2007, Hu et al. pointed out that Chien and Chen scheme also has some problems; it is Strong masquerading server/user attack, Restricted replay attack, Denial of service attack. it also slow wrong password detection, and proposed a new scheme. In 2008, Bindu et al. repeatedly pointed out on Chien and Chen scheme and proposed their scheme. However, we point out that all of their scheme also has some problems; it is not to protect the user anonymity and Denial of service attack. In addition, Bindu et al. is vulnerable to Strong masquerading server/user attack. Therefore, we demonstrate that their scheme also have some problems; it is the user anonymity and denial of service attack as above.

Key Words : Authentication, Smartcards, Anonymity, DoS attack

요 약 2004년에 Das 등은 사용자의 익명성을 보장하기 위한 원격 사용자 인증 구조를 제안했다. 2005년에 Chien 등이 Das 구조는 사용자의 익명성을 보장하지 못한다는 문제점을 제기하고 새로운 구조를 제안하였다. 2007년에 Hu 등은 Chien과 Chen 구조도 강한 서버/사용자 가장 공격, 제한된 재전송 공격, 서비스거부 공격 등과 같은 공격에 취약하며, 잘못된 패스워드의 탐지가 늦다는 문제점을 제기하고 새로운 구조를 제안했다. 2008년에는 Bindu 등이 Chien과 Chen 구조에 대해서 강한 서버/사용자 가장 공격에 대한 문제점을 제기하고 그 문제점을 해결하기 위한 새로운 구조를 제안하였다. 그러나 우리는 Hu et al. 구조와 Bindu et al. 구조 모두 사용자 익명성과 서비스 거부 공격에 대하여 취약하다는 것을 보였다.

1. Introduction

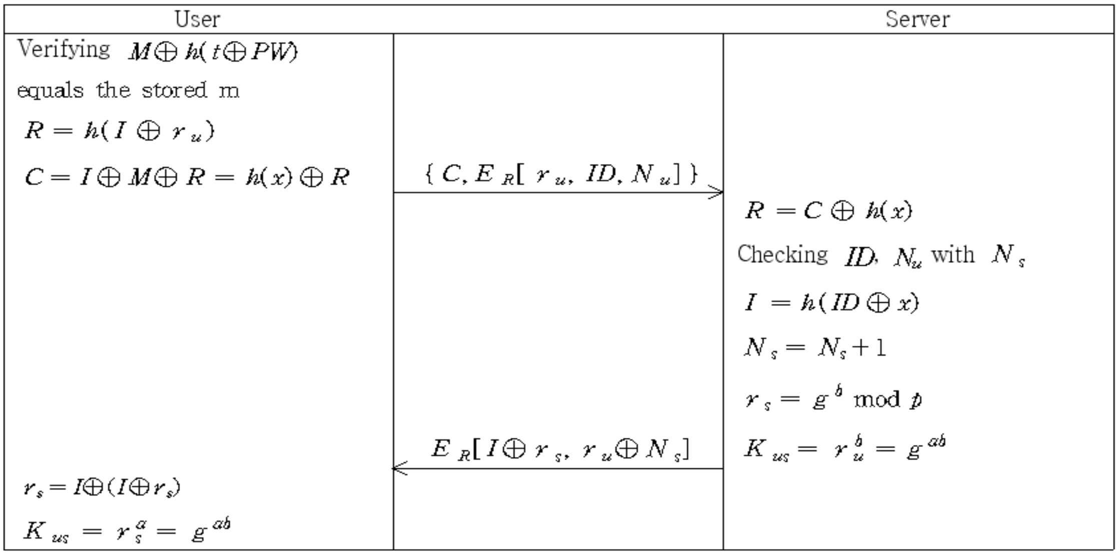
In 2004, Das et al.[1] proposed a remote authentication scheme to authenticate users while preserving the user anonymity. Their scheme adopted dynamic identification to achieve this function. Several schemes and improvements for remote user authentication schemes using smart cards [2-7] have been proposed. Then in 2005, Chien and Chen[8] pointed out Das et al. scheme fails to protect the user anonymity and proposed a new remote authentication scheme preserving user anonymity. In 2007, however, Hu et al.[9] pointed out that Chien and Chen scheme also has some problems; it cannot resist strong masquerading server/user attack, insider attack, denial of service attack and restricted replay attack; it also has the problem of slow wrong password detection. In 2008, Bindu et. al.[10] repeatedly pointed out that Chien and Chen scheme has problems. Therefore they proposed their scheme respectively.

However, In this paper we show that the Hu et al. and the Bindu et al. Scheme are vulnerable on User Anonymity and Denial of service attack.

The remainder of the paper organized as follows: Section 2 reviews of the Hu et al. and Bindu et al. Scheme, Section 3 analyze on the Hu et al. and the Bindu et al. Finally, section 4 gives a brief conclusion.

[1]Professor, Dept. of Information Security, Tong-Myoung University
[2]Professor, Division of Information & Communication Engineering, Baekseok University
[*]Corresponding Author : Seungsoo Shin(shinss@tu.ac.kr)

Received January 19, 2009 Revised February 16, 2009 Accepted February 18, 2008



User		Server
Verifying $M\oplus h(t\oplus PW)$ equals the stored m $R = h(I \oplus r_u)$ $C = I\oplus M\oplus R = h(x)\oplus R$	$\{C, E_R[r_u, ID, N_u]\}$ →	
		$R = C\oplus h(x)$ Checking ID, N_u with N_s $I = h(ID\oplus x)$ $N_s = N_s + 1$ $r_s = g^b \bmod p$ $K_{us} = r_u^b = g^{ab}$
$r_s = I\oplus(I\oplus r_s)$ $K_{us} = r_s^a = g^{ab}$	← $E_R[I\oplus r_s, r_u\oplus N_s]$	

[Fig. 1] Hu et. al Scheme

2. Review of the Hu et al. and the Bindu et al. Scheme

In this section, we review the Hu et. al. and the Bindu et al. scheme[4]. This scheme is composed of 3 phases namely the registration phase, the login phase and authentication phase. These phases are described in Fig. 1 as follows : The notations used throughout this paper are as follows:

[Table 1] Parameters

Symbol	Description
U, U_i	the general user
ID, ID_i	the identity of user U and U_i respectively.
PW, PW_i	the password of user U and U_i respectively.
S	the remote system
x	the strong secret key of S
$h()$	a secure one-way hash function
p, g	the parameters of Diffie-Hellman key exchange protocol
$\oplus$	the exclusive-or (XOR) operation
→	common channel transfer.
⇒	secure channel transfer.
$E_k[x]$	Encryption of x using key k
$D_k[x]$	Decryption of x using key k

2.1 Hu et al. Scheme

[Registration phase]

This phase is invoked whenever U initially registers or re-registers to S

Step R1 : $U \Rightarrow S$: ID, $h(t\oplus PW)$.

Step R2 : S computes $I = h(ID\oplus x)$, $M = I\oplus h(x)$ and $m = M\oplus h(t\oplus PW)$ $= h(ID\oplus x)\oplus h(x)\oplus(t\oplus PW)$.

Step R3 : $S \Rightarrow U$: a smart card containing ID, m, I, M and the public parameters $(h(\ ), p)$.

Step R5 : U enters t into his/her smart card.

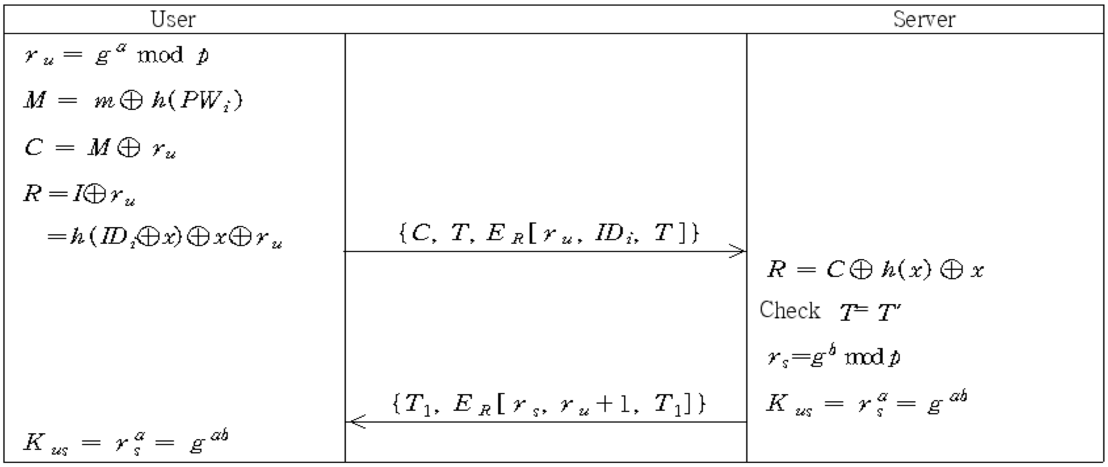
[Login phase]

This phase is invoked whenever U wants to login S

Step L1 : After checking the validity of the ID and verifying $M\oplus h(t\oplus PW)$ equals the stored m the smart card generates a random number $r_u = g^a \bmod p$, then computes $R = h(I\oplus r_u)$ and

$$C = I\oplus M\oplus R = h(x)\oplus R.$$

Step L2 : $U \rightarrow S$: $\{C, E_R[r_u, ID, N_u]\}$,


User
Server
$r_u = g^a \bmod p$
$M = m \oplus h(PW_i)$
$C = M \oplus r_u$
$R = I \oplus r_u$
$= h(ID_i \oplus x) \oplus x \oplus r_u$
$\{C,\ T,\ E_R[r_u,\ ID_i,\ T]\}$
$R = C \oplus h(x) \oplus x$
Check $T = T'$
$r_s = g^b \bmod p$
$K_{us} = r_s^a = g^{ab}$
$\{T_1,\ E_R[r_s,\ r_u + 1,\ T_1]\}$
$K_{us} = r_s^a = g^{ab}$

[Fig. 2] Bindu et. al. Scheme

[Authentication phase]

This phase is invoked whenever S receives $U'S$ login request.

Step A1 : S computes $R = C \oplus h(x)$, then decrypts $E_R[r_u,\ ID,\ N_u]$

Step A2 : After checking the validity of the ID, S compares the decrypted data N_u with the corresponding N_s.

Step A3 : S computes $I = h(ID \oplus x)$ and verifies whether the following equation holds: $R = h(I \oplus r_u)$. then S compute $K_{us} = r_u^b = g^{ab}$.

Step A4 : $S \rightarrow U$: $E_R[I \oplus r_s,\ r_u \oplus N_s]$, where $r_s = g^b \bmod p$.

Step A5 : U checks whether decrypted data contains the value $r_u \oplus (N_u + 1)$. U can generate the session key

$$K_{us} = r_s^a = g^{ab}.$$

2.2 Bindu et al. Scheme

The scheme is divided into three phases: the registration phase, the login phase and authentication.

[Registration phase]

Step R1 : U => S : ID_i? $h(PW_i)$

Step R1 : S Computes

$$m = h(ID_i \oplus x) \oplus h(x) \oplus h(PW_i)$$

and $I = h(ID_i \oplus x) \oplus x$.

Step R2 : S => U: the smart card containing m, I and the public parameters $(h(\ ),\ p)$.

[Login phase]

Step L1 : Generate a random number

$$r_u = g^a \bmod p.$$

Step L2 : Compute $M = m \oplus h(PW_i)$.

Step L3 : Compute $C = M \oplus r_u$.

Step L4 : Compute

$$R = I \oplus r_u = h(ID_i \oplus x) \oplus x \oplus r_u$$

Step L5 : U-> S :

$$\{C,\ T,\ E_R[r_u,\ ID_i,\ T]\}.$$

[Authentication phase]

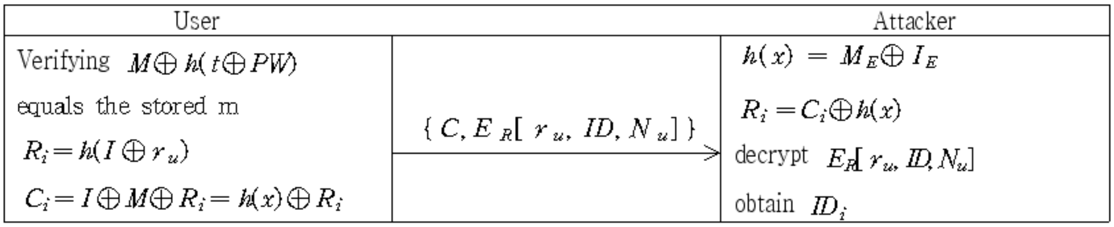
Step A1 : Computes $R = C \oplus h(x) \oplus x$, then decrypt $E_R[r_u,\ ID,\ T]$.

Step A2 : Check $T' - T \leq T'$

Step A3 : S -> U:

$$\{T_1,\ E_R[r_s,\ r_u + 1,\ T_1]\}$$

Step A4 : U checks whether the decrypted data contains $r_u + 1$. And then U computes



User		Attacker
Verifying $M\oplus h(t\oplus PW)$ equals the stored m $R_i=h(I\oplus r_u)$ $C_i=I\oplus M\oplus R_i=h(x)\oplus R_i$	$\{C, E_R[r_u, ID, N_u]\}$ →	$h(x) = M_E\oplus I_E$ $R_i=C_i\oplus h(x)$ decrypt $E_R[r_u, ID, N_u]$ obtain ID_i

[Fig. 3] User anonymity attack at Hu et. al

$$K_{us} = r_s^a = g^{ab}.$$

Step A5 : $U\text{->}S$: $E_{K_{us}}[r_s+1]$.

Step A6 : S checks whether it is equal to r_s+1 or not.

3. Analysis of the Hu et al. and the Bindu et al. Scheme

In this section, we explained attack method at Hu et al. and Bindu et al.

3.1 Hu et al. scheme

Hu et al. scheme has some problems; it is user anonymity and DoS attack. We explained these attack at Hu et al. scheme with figure 3.

3.1.1 User Anonymity

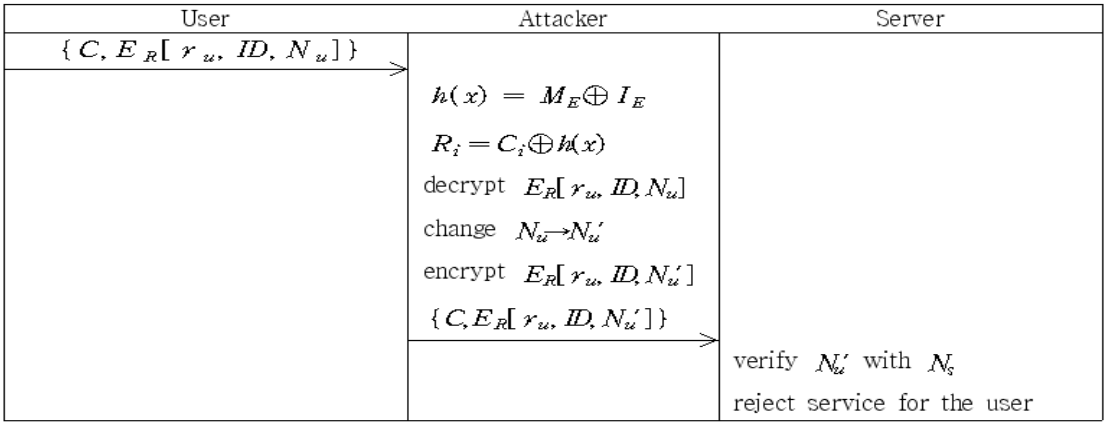
Hu et al. scheme explicitly demonstrated that their scheme protect Strong masquerading server/user attack. However, anyone can know a own user of a login request message in Hu et al. scheme, since the scheme fail to catch security of secret key R. Hence we show that Hu et al. scheme dose not protected user anonymity as Fig. 3. And then the user's ID is informed to anyone as follow.

Note that smart cards contain ID, m, I, M and the public parameters $(h(\ ), p)$ as we saw in Step R4 in Hu et al. scheme,

Step 1 : The attacker computes $R_E = h(I_E\oplus r_E)$ and $C_E = I_E\oplus M_E \oplus R_E = h(x)\oplus R_E$ from the attacker's smart card by oneself.

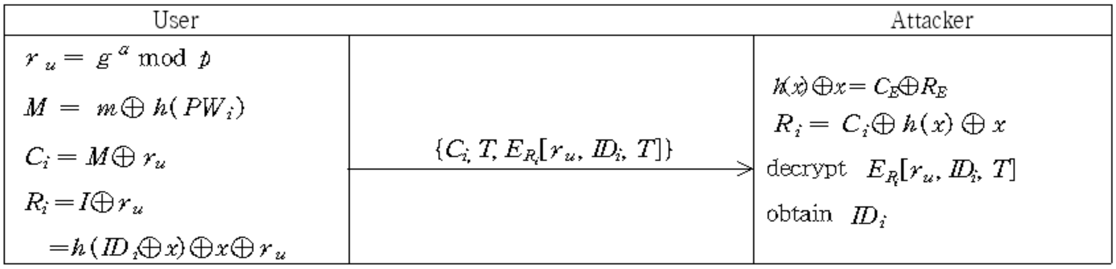
Step 2 : The attacker obtains $h(x)$ as $h(x) = C_E\oplus R_E$ or $h(x) = M_E\oplus I_E$.

Step 3 : The attacker can compute the secret key R_i of a user as $R_i = C_i\oplus h(x)$, after intercepting and blocking the message of the user in Step L3 to the server.



User	Attacker	Server
$\{C, E_R[r_u, ID, N_u]\}$ →		
	$h(x) = M_E\oplus I_E$ $R_i=C_i\oplus h(x)$ decrypt $E_R[r_u, ID, N_u]$ change $N_u\rightarrow N_u'$ encrypt $E_R[r_u, ID, N_u']$ $\{C, E_R[r_u, ID, N_u']\}$ →	
		verify N_u' with N_s reject service for the user

[Fig. 4] DoS attack at Hu et. al



User		Attacker
$r_u = g^a \bmod p$ $M = m\oplus h(PW_i)$ $C_i = M\oplus r_u$ $R_i = I\oplus r_u$ $= h(ID_i\oplus x)\oplus x\oplus r_u$	$\xrightarrow{\{C_i, T, E_{R_i}[r_u, ID_i, T]\}}$	$h(x)\oplus x = C_E\oplus R_E$ $R_i = C_i\oplus h(x)\oplus x$ decrypt $E_{R_i}[r_u, ID_i, T]$ obtain ID_i

[Fig. 5] User anonymity at Bindu et. al

The attacker can acquire the user's ID. And he/she can know and guess the own user of the ID.

3.1.2 Denial of service attack

We mentioned that these scheme inform anyone the correct value of secret key R. We show that this scheme is vulnerable on DoS attack as Fig. 4. And then the attacker can compute as follow.

Step 1 : The attacker intercepts and blocks the login request message of the user $\{ C, E_R[r_u, ID, N_u] \}$ in Step L3.

Step 2 : The attacker decrypts the message $E_R[r_u, ID, N_u]$ and changes N_u'.

Step 3 : The attacker encrypts the message $E_R[r_u, ID, N_u']$ and sends $\{ C, E_R[r_u, ID, N_u] \}$ to the server.

Step 4 : The server sends a synchronization signal to the user. Note that the user must sends N_u with N_s.

The attacker forges N_u to the server. Therefore, the server cannot but reject the message.

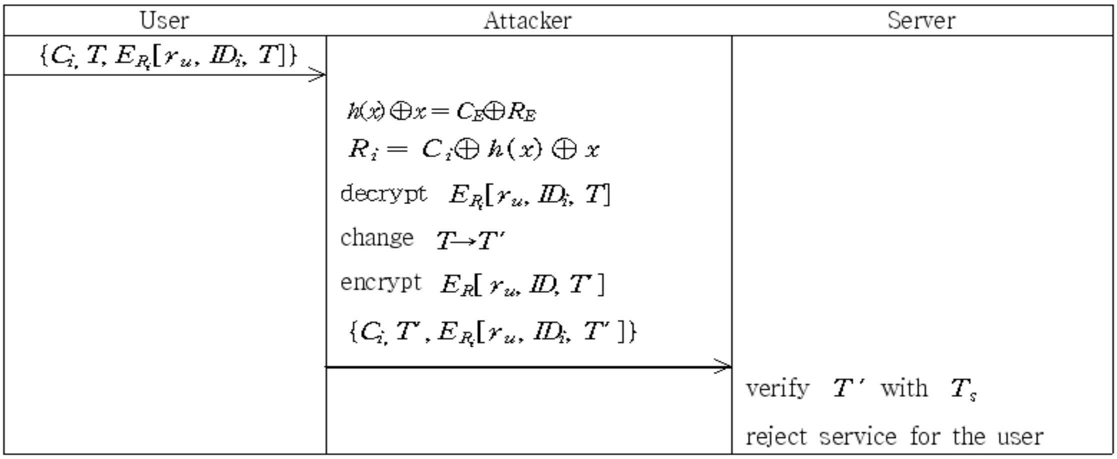
3.2 Bindu et al. scheme

Bindu et al. scheme also has some problems; it is user anonymity and DoS attack. We explained these attack at Bindu et al. scheme with figure.

3.2.1 User Anonymity

Similarly, Bindu et al. also drop the user's ID to anyone as Fig. 5. Note that the smart card of the attacker contains m, I and the public parameters $(h(\ ), p)$.

Step 1 : The attacker computes $M_E = m_E\oplus h(PW_E)$, $C_E = M_E\oplus r_E$ and



User	Attacker	Server
$\xrightarrow{\{C_i, T, E_{R_i}[r_u, ID_i, T]\}}$		
	$h(x)\oplus x = C_E\oplus R_E$ $R_i = C_i\oplus h(x)\oplus x$ decrypt $E_{R_i}[r_u, ID_i, T]$ change $T\rightarrow T'$ encrypt $E_R[r_u, ID, T]$ $\{C_i, T', E_{R_i}[r_u, ID_i, T']\}$ $\longrightarrow$	
		verify T' with T_s reject service for the user

[Fig. 6] DoS attack at Bindu et. al.

$R_E = I_E \oplus r_E = h(ID_E \oplus x) \oplus x \oplus r_E$ from his/her smart card by oneself.

Step 2 : The attacker obtains $h(x) \oplus x$ as $h(x) \oplus x = C_E \oplus R_E$ or $h(x) = M_E \oplus I_E$.

Step 3 : The attacker can compute the secret key R_i of a user as $R_i = C_i \oplus h(x) \oplus x$, after intercepting and blocking the message of the user in Step L3 to the server.

The attacker can acquire the user's ID And he/she can know and guess the own user of the ID.

3.2.2 Denial of service attack

As the same, Note that Bindu et al. scheme also inform anyone the correct value of the secret key R. And then, the attacker can perform as follow in Fig. 6.

Step 1 : The attacker intercepts and blocks the login request message of the user $\{C, T, E_R[r_u, ID_i, T]\}$ in Step L4.

Step 2 : The attacker decrypts the message $E_R[r_u, ID, T]$ and changes T_E

Step 3 : The attacker encrypts the message $E_R[r_u, ID, T_E]$ and sends $\{C, T_E, E_R[r_u, ID_i, T_E]\}$to the server.

The server checks the validity of T_E and reject the login message of the user.

4. Conclusion

All of the schemes that have been proposed up to the present fail to completely conquer the problems as above, although communication used smart card is increasing on network. In order to be secure by network, we need the scheme that can conquer these mentioned problems for efficient authentication and smoothly preserving the service to the user. To archive the scheme, we need a secret key that can be known only to the user and the server by public key but the attacker, with considering on public key and secret key. In order to use protocols using smart cards, the protocols have to provide user anonymity and overcome DDoS attack, because of user information is considered as privacy, therefore user anonymity attack threats privacy of users and DDoS attack can kill server providing service.

References

[1] M. L. Das, A. Saxena, 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.

[2] Amit. K. Awasthi and Sunder Lal, "A Remote User Authentication with Forward Secrecy," IEEE Transactions on Consumer Electronics, Vol.49, No.4, pp. 1246-1248, 2003.

[3] C. Chang, and T. Wu, "Remote Password Authentication with Smart Cards," IEEE Proceedings Computers and Digital Techniques, Vol.138, No.3, pp. 165-168, 1991.

[4] C. Chang, and S. Hwang, "Using Smart Cards to Authenticate Remote Passwords," Computers and Mathematics with Application, Vol.26, No.7, pp. 19-27, 1993.

[5] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics.

[6] H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authen- tication: Smart Card," Computers and Security, Vol. 21, No. 4, pp. 372-375, 2002.

[7] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "Security Enhancement for a Dynamic ID-based remote user Authentication Scheme," Proceedings of the intern national conference on Next Generation Web Services Practices (NWeSP'"05) 2005.

[8] Hung-Yu Chien and Che-Hao Chen, "A Remote Password Authentication Preserving User Anonymity," Proceedings of the 19th International Conference on Advanced Infor mation Networking and Applications, (AINA '"05), 2005.

[9] Hu, Yang and Niu, "Improved Remote User Authentication Scheme Preserving User Anonymity," IEEE CNSR'07, 2007.

[10] Mrs. C. Shoba Bindu, Dr P. Chandra Sekhar Reddy, and Dr B. Satyanarayana, "Improved remote

user authentication scheme preserving user anonymity," International Journal of Computer Science and Network Security, Vol.8 No.3, March 2008.

Jong-Seok Choi [Associate member]

- Mar. 2004 ~ Present : Student in Department of Information Security from Tong-Myoung University

<Research Interests>
Cryptographic Protocol, USN.

Seung-Soo Shin [Regular member]

- Mar. 2005 ~ Present : Professor, Tong-Myoung University.
- Aug. 2004 : Chungbuk National University (Ph.D.).

<Research Interests>
Cryptographic Protocol, Wireless PKI, Network Security, USN. Smartcards

Kun-Hee Han [Life member]

- Mar. 2001 ~ Present : Professor, Division of Information & Communication Engineering, Baekseok University

<Research Interests>
RFID, Network Security, USN, Wireless PKI