International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.155-164
http://dx.doi.org/10.14257/ijsia.2013.7.6.16

Enhanced Smartcard based Multi-Server Authentication Scheme

Hee-Joo Park[1] and Chonggun Kim[2]

[1]*Dept. of Cyber Security, Kyungil University*
[2]*Dept. of Computer Engineering, Yeungnam University*
[1]*hjpark@kiu.ac.kr*, [2]*cgkim@yu.ac.kr*

Abstract

Generally, if a user wants to use numerous different network services, he/she must register himself/herself to every service providing server. It is not easy task for users to remember these different identities and passwords for each server. To solve the problem, various multi-server authentication schemes have been proposed. Recently, Wang et al. proposed a smartcard based multi-server authentication scheme. They claimed that their scheme is secure against impersonation attack, server spoofing attack and offline dictionary attack, and provides forward secrecy. However, through careful analysis, we find that Wang et al.'s scheme is still vulnerable to password guessing attack with stolen smartcard. Furthermore, we propose an enhanced smartcard based multi-server authentication scheme to cope with the security problem in Wang et al.'s scheme. The proposed scheme is suitable for use in distributed multi-server architecture since it provides mutual authentication, efficiency and security.

Keywords: *We would like to encourage you to list your keywords in this section*

1. Introduction

With the rapid development of Internet and electronic commerce technology, many life convenient services are provided through Internet such as online shopping, online game, cloud computing, distributed electronic medical records system, *etc*. Recently, more and more people have relied on computer networks to exchange knowledge, access information and process data in distributed network environments, and therefore network security has becoming very important. Various methods have been devised to frustrate different attack attempts of the sensitive information stored in servers. Password based authentication is the most accepted and widely adopted mechanism because of its low-cost, easy-operation and simple-implementation advantages [1-20]. Traditionally, password based authentication is mostly considered in single server environments [1-5]. Nevertheless, it has not been efficiently solved in a multi-server based environment. The objective of multi-server based environment emphasizes that any user can obtain service granted from multiple servers without repeating registration to each server. In fact, with the rapid growth of computer networks, many network environments including Ethernet [6], Distributed networks [7-8], and wireless networks [9-10], have been becoming multi-server based.

In order to solve the problem of multi-server environments, Li *et al.*, proposed a remote user authentication scheme using neural networks, which can be compatible with multi-server network architecture without repetitive registrations [11]. However, Li *et al.*, scheme requires high communication and computation costs since each user must have large memory to store public parameters for authentication. For tackling the

ISSN: 1738-9976 IJSIA

efficiency problem of Li *et al.*, scheme, Juang proposed an efficient multi-server key agreement protocol based on the hash function and the symmetric key cryptosystem [12]. But, Chang *et al.*, showed that Juang's protocol has lack of efficiency since the computation and storage overheads of each user are proportional to the number of users and servers. Furthermore, if the secret value of the smartcard is extracted by some way, Juang's protocol is vulnerable to offline password guessing attack [13]. To improve the shortcomings, Chang *et al.*, proposed a novel remote user authentication protocol, which was found vulnerable to insider attack, spoofing attack and registration center spoofing attack. Tsaur et al. proposed a multi-server authentication protocol based on the RSA cryptosystem and Lagrange interpolation polynomial [14]. However, Tsaur *et al.*, protocol is also not efficient because it needs high communication and computation overheads. Tsai also proposed an efficient multi-server authentication protocol without using verification table, which is based on nonce and one-way hash function [15]. Tsai's protocol is very suitable to be used in the distributed network environment because of their low computation costs. A list of security requirements for the multi-server architecture has been proposed in [16] to guide the further design of the authentication schemes as following: (1) single registration, (2) verification table free, (3) ability to update password freely and securely, (4) mutual authentication and key management, (5) low computation cost with strong security. Many authentication schemes such as those in [12–19] have been proposed to try to fulfill above mentioned requirements. The schemes in [12, 16] and [17] fail under impersonation attacks and server spoofing attacks conducted by insiders. Wang et al.'s scheme is robust against both the impersonation attacks and the server spoofing attacks, but fails to hold forward security [18]. Geng *et al.*, scheme possesses robustness against all above mentioned attacks, but is prone to cryptographic algorithm cracking attacks [19]. Recently, Wang *et al.*, in [20] also proposed a smartcard based efficient and secured multi-server authentication scheme and argued that their scheme is robust against all discussed malicious attacks with high efficiency.

Unfortunately, this paper points out that Wang *et al.*, scheme does not provide security against the offline password guessing attack with lost smartcard and proposes an enhanced multi-server authentication scheme to solve the security problem in Wang et al.'s scheme. Security breach possibility in smartcard of Want et al.'s scheme is discussed first and then security analysis for it is provided focused on the attack. The proposed scheme uses not only password and smartcard but also biometric information to enhance the security of the authentication scheme.

This rest of the paper is organized in the following way. Section 2 reviews Wang et al.'s multi-server authentication scheme. Security analysis is given focused on the password guessing attack of Wang et al.'s scheme in section 3. In section 4, an enhanced multi-server authentication scheme is proposed to solve the security problem in Wang et al.'s scheme. Section 5 provides security and efficiency analyses between the proposed scheme and the related previous schemes. Finally, section 6 concludes the paper.

2. Wang et al.'s Multi-Server Authentication Scheme

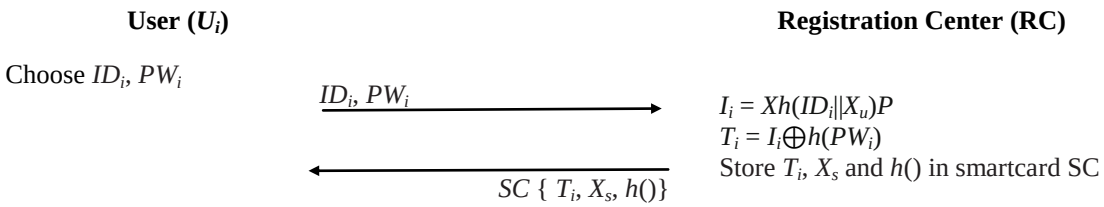
This section reviews Wang et al.'s smartcard based efficient and secured multi-server authentication scheme [20]. Their scheme is composed of four phases including initialization phase, registration phase, authentication phase and password changing phase. We will only simply review the registration phase and the authentication phase,

which would be focused on the security analysis part. First of all, we review all the notifications used in this paper as shown in Table 1.

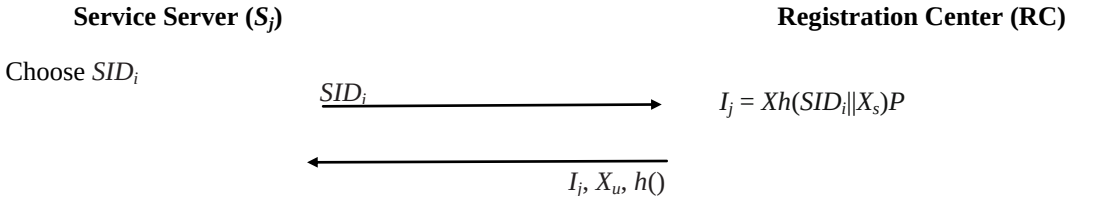
Table 1. Notations

Notation	Description
U_i	The *i*-th user
ID_i	The identity of the *i*-th user
PW_i	The password of the *i*-th user
b_i	The biometric information of the *i*-th user
S_j	The *j*-th server
SID_j	The identity of the *j*-th server
I_i	The identity value of the *i*-th agent
P_i	The particular value of the *i*-th agent
P	The generator of a cyclic group
G	The cyclic group generated by P
SC	It denotes for smartcard that a user holds
p	A large prime number
$h(\cdot)$	A one-way hash function whose output is element of the addict cyclic group
X	Mater secret key
X_u	User secret key
X_s	Server secret key
$\oplus$	Exclusive or operation
$\|\|$	Concatenation operation
$E_{key}(\cdot)$	Encryption function using the key "key"
RC	Registration center of the system, which is the only trusted party
RPS	Redundant key Protected Scheme, which is our proposal

Figures 1 and 2 show the registration phase and the authentication phase.



(a) User registration



(b) Service server registration

Figure 1. Registration Phase

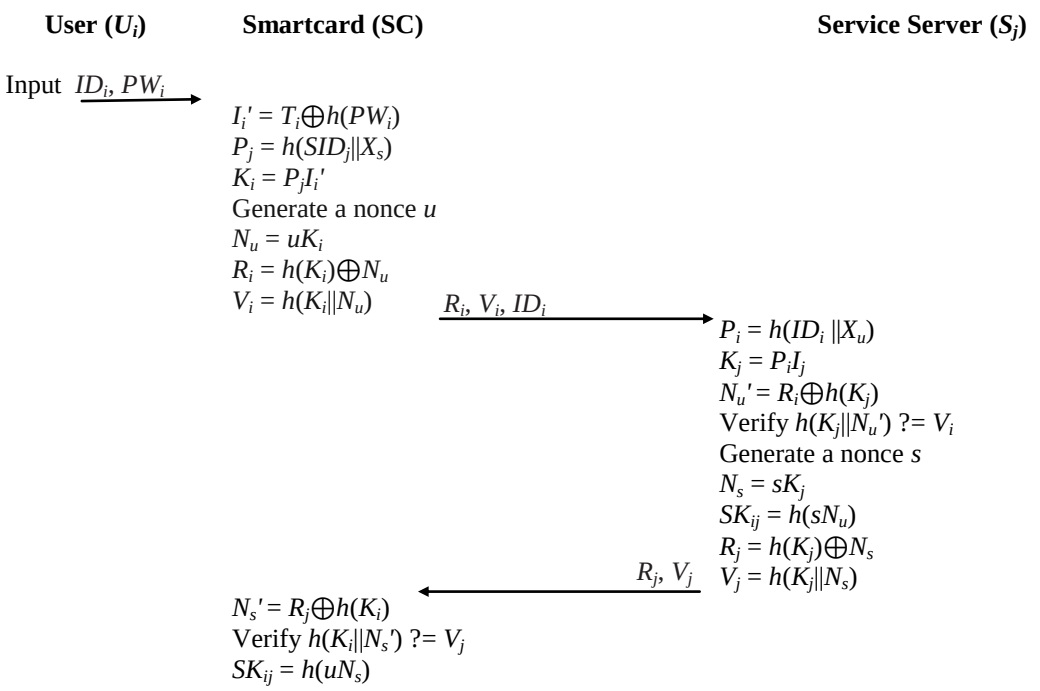


Figure 2. Authentication Phase

3. Security Analysis of Wang et al.'s Multi-Server Authentication Scheme

This section shows that Wang et al.'s smartcard based efficient and secured multi-server authentication scheme does not provide security against the offline password guessing attack with lost smartcard. Security breach possibility in smartcard is discussed first and then security analysis is provided focused on the attack.

3.1. Information Breach in Smartcard

According to the researches in [21, 22], most of the existing smartcards are vulnerable as sensitive verifier and secret values stored in the smartcards could be extracted by monitoring their power consumption. Thus, weaknesses of the authentication schemes using smartcard are mainly due to two problems. First, if an adversary obtains a legal user's smartcard even without the corresponding password, he/she can use it to product a fabricated login message, and then impersonate the user to pass the authentication. Secondly, if the adversary captures a server's secret key and smartcard at the same time, he/she can easily impersonate the legitimate user to login the remote system. Due to above reasons, most of the existing schemes using smartcard are still vulnerable to password guessing attack with lost smartcard.

3.2. Offline Password Guessing Attack with Lost Smartcard

Since the login request message from the legal user is sent to the server through an insecure channel, we could assume that attacker can control the channel completely. That is to say, attacker can intercept the valid authentication message $\{ID_i, R_i, V_i\}$ of the user from the channel. Then attacker can compute $I_i' = T_i \oplus h(PW_i')$ with the guessed password PW_i' and T_i from the stolen smartcard, $P_j' = h(SID_j||X_s)$ with SID_j and X_s from

the stolen smartcard, $K_i' = P_j'I_i'$, $N_u' = R_i \oplus h(K_i')$ and $V_i' = h(K_i'||N_u')$, and verifies V_i' with the intercepted V_i by using offline password guessing attack by following the steps

[Step 1] An attacker intercepts a legal authentication message $\{ID_i, R_i, V_i\}$ from a legal user and steals the user's smartcard.
[Step 2] The attacker chooses a password candidate PW_i' from dictionary.
[Step 3] Using the known value T_i, SID_j and X_s from the smartcard, the attacker computes $I_i' = T_i \oplus h(PW_i')$, $P_j' = h(SID_j||X_s)$, $K_i' = P_j'I_i'$, $N_u' = R_i \oplus h(K_i')$ and $V_i' = h(K_i'||N_u')$.
[Step 4] The attacker verifies if the computed value V_i' is equal to V_i on the smartcard. If they are equal, the attacker could make sure that his/her guess is right. Otherwise, the attacker repeats the whole guessing process again and again until the correct one come out.

4. Enhanced Smartcard based Multi-Server Authentication Scheme

This section proposes an enhanced multi-server authentication scheme to solve the security problem in Wang et al.'s scheme. The proposed scheme uses not only password and smartcard but also biometric information to enhance the security of the scheme. There are four phases in the proposed scheme - the initialization phase, the registration phase, the authentication phase and the password change phase, which would use the similar basic building block with Wang et al.'s scheme.

The multi-server architecture is designed to fulfill the increasing demands and to cover expanding service areas by establishing multiple servers to provide identical services. In the multi-server systems, registration center (RC), users with smartcard (SC) and servers play the major roles. The RC is the only trusted party in the system which registers users and authorizes servers. The servers provide identical services to the registered users while the users gain services from these servers.

4.1. Initialization Phase

In this phase, the RC establishes an additive cyclic group G whose order is a large prime p with a generator P. Then, the RC finds a cryptographic hash function $h()$ whose input can either be or not be an element of G. The RC generates X, X_u and X_s, where X is the master secret key which is only known to the RC, X_u is the user secret key which is only known to servers and X_s is the server secret key which is known to users.

For each server S_j, the RC computes its identity value $I_j = Xh(SID_j||X_s)P$, and passes I_j, $h()$, and X_u to the server S_j through a secure channel. It has to be mentioned that I_j is not just computed by multiplying X, $Xh(SID_j||X_s)$ with P but by modular multiplying $h(SID_j||X_s)$ with P and then modular multiplying X with $h(SID_j||X_s)P$. The outcome is an element in the additive group G, which only has finite number of elements with restrained data length. All non-G-element values e.g. outcomes of hash functions, are the integers that can be used to produce elements in G by modular multiplying other elements in G such as P. This computation will introduce the protection from Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP states that, for equation $Q = sP$ where $Q, P \in G$ and s is an integer, it is easy to get Q when s and P are known and difficult to get s when Q and P are known. Another point to be noted is that the elements in G, as most of the values used in the scheme, cannot be applied to exclusive-or operations (XOR). But due to the fact that all information stored in computer systems are bit strings and the information in binary format can be interpreted differently with different interpretation method, such values are interpreted as bit-strings when XOR

operations are performed. All the values are XORed before transmission and will be recovered immediately after them received. All processing on these values are in their original form, and data-type mismatch will occur only in the unauthorized session.

4.2. Registration Phase

In this phase, a user selects his/her identifier ID_i and password PW_i, inputs biometric information b_i and sends $\{ID_i, PW_i, b_i\}$ to the RC. The RC computes the identity value of the user $I_i = Xh(ID_i||X_u)P$, the test value $T_i = I_i \oplus h(PW_i)$ and the amplified biometric value $B_i=h(ID_i||b_i)$. After that, the RC passes the user's smartcard through a secure channel after storing $\{T_i, X_s, B_i, h()\}$ into it.

4.3. Authentication Phase

When the user wants to be serviced from the server, he/she enters his/her identity ID_i, the server's identity SID_j, the password PW_i and the biometric information b_i with the following steps:

[Step 1] The SC computes $B_i'=h(ID_i||b_i)$ and verifies whether $B_i'=B_i$. If the verification fails, the user has no authority to use the SC and the SC terminates the scheme. Otherwise, the SC computes $I_i' = T_i \oplus h(PW_i)$, $P_j = h(SID_j||X_s)$, and $K_i = P_j I_i'$. The SC generates a nonce u and computes $N_u = uK_i$. A requesting message $R_i = h(K_i) \oplus N_u$ is computed with the verification message $V_i = h(K_i||N_u)$. After that, the SC sends a message containing ID_i, R_i and V_i to the server.

[Step 2] Upon receiving the message from the user, the server computes the particular value of the requesting user $P_i = h(ID_i||X_u)$, the master key $K_j = P_i I_j$, and $h(K_j)$. After getting N_u' from R_i by $N_u' = R_i \oplus h(K_j)$, the server verifies the verification message whether $h(K_j||N_u') = V_i$. If the user fails to pass the verification, the server discards the message. Otherwise, the server generates a nonce s, computes $N_s = sK_j$ and installs a session key $SK_{ij} = h(sN_u)$. Then, the server computes the responding message $R_j = h(K_j) \oplus N_s$ with the verification message $V_j = h(K_j||N_s)$. The server sends a message containing R_j and V_j back to the user.

[Step 3] Upon the user gets R_j and V_j from the server, he/she gets N_s' from R_j by $N_s' = R_j \oplus h(K_i)$ and verifies the verification message whether $h(K_i||N_s') = V_j$. If the verification fails, the user discards the message. Otherwise, the user installs a session key $SK_{ij} = h(uN_s')$.

Then the user is able to communicate with the server within a period. If the server cannot receive messages from the user before timeout, the server will deny this session and uninstall the session key.

4.4. Password Changing Phase

When user wants to change the password, he/she can change his/her password freely and completely locally without help of the RC. This phase contains the following steps:

[Step 1] The user inputs his/her SC into the card reader of a specific terminal and provides his/her identifier ID_i, biometric information b_i, old password PW_i^{old} as well as new password PW_i^{new}. After that the SC computes $B_i'=h(ID_i||b_i)$.

[Step 2] The SC verifies whether $B_i' = B_i$. If the verification fails, this means that the user has no right to use the SC and entered incorrect biometric information b_i and hence, it terminates the phase immediately.

[Step 3] Otherwise, the SC computes $T_i^{new} = T_i^{old} \oplus PW_i^{old} \oplus PW_i^{new}$ and replaces T_i^{new} into T_i^{old} in the memory of the SC.

5. Security and Efficiency Analyses

This section provides security and efficiency analyses of the proposed scheme by providing comparisons with related authentication schemes in [15, 16, 20]. We first show that the proposed scheme can resist against the impersonation attack, server spoofing attack, and offline password guessing attack, and provide forward secrecy. Then we will provide efficiency analysis focused on the communication cost and the computation cost.

5.1. Security Analysis

This section provides security analysis of the proposed scheme. We show that the proposed scheme can resist against the following attacks.

[S1] Impersonation attack: This is an attack where an attacker masquerades as a legal user. An inside attacker is supposed to be a legal user or a legal server. He/she masquerades to be another legal user to get services from other servers. The inside attacker will gain free services from the servers while the masqueraded user will be charged, causing losses of service provided to the corresponding legal users. The proposed scheme has the following way to prevent impersonation attacks as follows: (1) Store values in the SC, which is derived from the user key and keeps it secret, i.e. $\{T_i, X_s, B_i\}$ (2) Send request message which is a derived from the user value, i.e. $\{R_i, V_i\}$ (3) Verify this message with the claiming information of the requester by any agent in the system, which is able to verify the user value by examining the requesting message, i.e. $\{V_i\}$. The rationale of the above operations is that the only way to verify the identity of an entity is to verify a pre-stored value which is held and only held by the entity itself.

[S2] Server spoofing attack: This is an attack where an attacker masquerades a legal server. The inside attacker is supposed to be a valid user or a valid server in the system. Server spoofing attacks conducted by an insider may cause a leaking of the confidential user information. The proposed scheme has the following way to prevent server spoofing attacks conducted by insiders formulated as follows: (1) Store a secret identification value of a server at the server and is only known by the server itself, i.e. $\{X_u\}$ (2) Use the server value to derive a verification message, i.e. $\{X_u\}$ (3) Verify this message with the claiming information of the requester identification by any agent which is able to verify the identification value in the requesting message, i.e. $\{X_u, SK_{ij}\}$. The rationale of the above operations is similar to that of the scheme to prevent impersonation attacks because they have the same goal to prevent the masquerading.

[S3] Offline password guessing attack: It refers to an action to crack passwords or other confidential information of a system with an offline dictionary which stores a pre-calculated table with/without the information on the smartcard. The way to prevent the offline guessing attacks is to integrate identity information or other confidential information in the system with a secret key, which can be referred as the RC key, which never be used explicitly after the system setting up. In the proposed scheme, no

one can get any system key related information from the offline dictionary. Since the redundant system key X is used in producing identity value of each entry and this key is never directly used in the authentication process, for each value of X, there is a valid value of X_u or X_s which can obtain the same identity value. Hence, with the offline dictionary, the intruder can only get a list of pairs of (X, X_u/X_s) instead of the exact X_u/X_s. To further identify the exact pair, the intruder has to either establish a connection or compromise another SC to know whether its guess is correct or not. If the intruder tries to crack PW_i from T_i, the intruder has to possess any verifiable value, which could tell the correct guess or not. Hence, the proposed scheme is robust against the offline guessing attacks.

[S4] Forward secrecy: An authentication scheme with the forward security will not expose the already derived session key even though the secret keys have been disclosed. To maintain this property, the session key should be protected by the cryptographic algorithms. In the proposed scheme, even though the intruder knows the master key of the session, it can only get $N_u = uK$ and $N_s = sK$. Thus, the nonce will still be protected by the ECDLP and the session key $SK = usK$ is further protected by the Computational Diffie-Hellman Problem (CDHP). Hence, the proposed scheme can support forward secrecy.

The security functionalities of each scheme have been listed and compared in Table 2. We can conclude that only the proposed scheme satisfies all the necessary security features from the table.

Table 2. Security Comparison between Related Authentication Schemes

Attack / Scheme	S1	S2	S3	S4
Tsai et al's scheme [15]	Robust	Prone	Prone	No
Liao et al.'s scheme [16]	Prone	Prone	Prone	No
Wang et al.'s scheme [20]	Robust	Robust	Prone	Yes
Proposed scheme	Robust	Robust	Robust	Yes

S1 – Impersonation attack; S2 – Server spoofing attack; S3 – Offline password guessing attack; S4 – Forward secrecy

5.2. Efficiency Analysis

The efficiency of security scheme is very important focused on the computation cost and the communication cost. We provide comparisons of related authentication schemes focused on those two costs in Table 3.

Table 3. Efficiency comparison between Related Authentication Schemes

Attack / Scheme	E1	E2
Tsai et al's scheme [15]	22T	1,644bits
Liao et al.'s scheme [16]	15T	896bits
Wang et al.'s scheme [20]	18T	640bits
Proposed scheme	18T	640bits

E1 – Total computation cost; E2 – Total communication cost

It is assumed that P and other elements in the cyclic group, ID_i, SID_i, PW_i, B_i, secret keys and the output from the hash functions are 128bits in length and the time costs of

hash functions, random generations, encryptions, decryptions and modulation multiplications are approximately the same as *T* for the simplicity of comparisons as the same as in [20]. Other operations like XOR and concatenation are supposed to take negligible time. The total time cost of each scheme is taken as the summation of the time taken at each step. For the time cost of communication, we only considered authentication phase, which is very important and most frequently used phase. From Table 3, it is clear that the proposed scheme has the same costs with Wang *et al.*, scheme, which is below the average. However, the password changing phase in our scheme requires no involvement of the registration server, which is the contrast with Wang et al.'s scheme.

6. Conclusion

Remote user authentication and key agreement scheme using smartcards is a very practical solution to validate the eligibility of a remote user and provide secure communication later. Also, due to fast progress of networks and information technology, most of provided services are in multi-server environments. To support the authentication for the multi-server environments, Wang *et al.*, proposed a smartcard based multi-server authentication scheme. However, this paper pointed out that their scheme is still vulnerable to the password guessing attack with lost smartcard, which is against with their claims. Furthermore, we proposed an enhanced smartcard based multi-server authentication scheme to solve the security problem in Wang *et al.*, scheme. The major merits of the proposed scheme include: (1) users only need to register at the registration centre once and can use permitted services in eligible servers; (2) the scheme does not need a verification table; (3) users can freely choose their passwords; (4) the computation and communication cost is very low; (5) servers and users can authenticate each other; (6) it generates a session key agreed by the user and the server; (7) it is a nonce-based scheme which does not have a serious time-synchronization problem; (8) users can change their password without helping of the registration center.

References

[1] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, vol. 24, **(1981)**, pp. 770-772.
[2] B. Menkus, "Understanding the use of passwords", Computers and Security, vol. 7, **(1988)**, pp. 132-136.
[3] C. Pfleeger, "Security in Computing", 2nd Edition, Prentice-Hall. **(1997)**.
[4] Y. An and Y. Joo, "Security Analysis and Improvements of a Password-Based Mutual Authentication Scheme with Session Key Agreement", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**, pp. 85-94.
[5] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang and D. Zou, "Efficient Password-based Two Factors Authentication in Cloud Computing", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 143-148.
[6] K. Lee, S. Lee and M. Lee, "Worst case communication delay of real-time industrial switched Ethernet with multiple levels", IEEE Transactions on Industrial Electronics, vol. 53, no. 5, **(2006)**, pp. 1669-1676.
[7] C. Hwang and C. Shih, "A distributed active-vision network-space approach for the navigation of a carlike wheeled robot", IEEE Transactions on Industrial Electronics, vol. 56, no. 3, **(2009)**, pp. 846-855.
[8] W. Juang, S. Chen and H. Liaw, "Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards", IEEE Transactions on Industrial Electronics, vol. 55, no. 6, **(2008)**, pp. 2551-2556.
[9] D. He, M. Ma, Y. Zhang, C. Chen and J. Bu, "A strong user authentication scheme with smart cards for wireless communications", Computer Communications, vol. 34, **(2011)**, pp. 367-374.
[10] C. Lee, M. Hwang and I. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments", IEEE Transactions on Industrial Electronics, vol. 53, no. 5, **(2006)**, pp. 1683-1687.

[11] L. H. Li, L. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks", IEEE Transactions on Neural Networks, vol. 12, no. 6, **(2001)**, pp. 1498–1504.
[12] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards", IEEE Transaction on Consumer Electronics, vol. 50, no. 1, **(2004)**, pp. 251–255.
[13] C. C. Chang and J. S. Lee J-S, "An efficient and secure multi-server password authentication scheme using smart cards", Proc. of the third international conference on cyberworlds, **(2004)**, pp. 417-422.
[14] W. J. Tsaur, C. C. Wu and W. B. Lee, "A smart card-based remote scheme for password authentication in multi-server Internet services", Computer Standards & Interfaces, vol. 27, no. 1, **(2004)**, pp. 39-51.
[15] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table", Computers & Security, vol. 27, no. 3-4, **(2008)**, pp. 115–121.
[16] Y. P. Liao and S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, vol. 31, no. 1, **(2009)**, pp. 24-29.
[17] Y. Lee and D. H. Won, "Security weaknesses in Chang and Wu's key agreement protocol for a multi-server environment", Proc. of the IEEE international conference on e-business engineering, **(2008)**, pp. 308-314.
[18] R. C. Wang, W. S. Juang and C. L. Lei, "User authentication scheme with privacy-preservation for multi-server environment", IEEE Communications Letters, vol. 3, no. 2, **(2009)**, pp. 157-159.
[19] J. Geng and L. Zhang, "A dynamic ID-based user authentication and key agreement scheme for multi-server environment using bilinear pairings", Proc. of Workshop on power electronics and intelligent transportation system, **(2008)**, pp. 33–37.
[20] B. Wang and M. Ma, "A smart card based efficient and secured multi-server authentication scheme", Wireless Pers. Commun., vol. 68, **(2013)**, pp. 361-378.
[21] P. Kocher, J. Jaffe and B. B. Jun, "Differential power analysis", Proc. of Advances in Cryptology 1999, **(1999)** pp. 388-397.
[22] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computer, vol. 51, no, 5, **(2002)**, pp. 541-552.

Authors

Hee-Joo Park, he is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the B.S. and M.S. degrees in Electrical Engineering from Yeungnam received the Ph.D. degree in Computer Science and Statistics from Catholic University of Daegu, Republic of Korea, in 1995. He had been a professor from 1982 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include information security, neural network, pattern recognition, ad-hoc network and sensor network.

Chonggun Kim, he is a professor at the Department of Computer Engineering, Yeungnam University, Korea from 1991. He received the B.S. and M.S. degrees in Electrical Engineering from Yeungnam University, Republic of Korea, in 1987 and 1991, respectively. He received the Ph.D. degree from University of Electro-Communications, Japan, in 1997. He was a visiting scholar at Virginia polytechnic University from 1996 to 1997 and was a visiting scholar at University of California Santa Cruz (UCSC) from 2003 to 2004. His research interests include distributed computing systems, computer networks, mobile networks, and performance evaluation.

