International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.419-428
http://dx.doi.org/10.14257/ijsia.2015.9.11.38

Anonymous Password-based Authenticated Key Agreement Scheme with Non-tamper Resistant Smart Cards

Yunghee Lee[1], Hyunsung Kim[2]

[1]*Dept. of Cyber Security,*
Kyungil University, Kyungsan, Kyungbuk 712-701, Korea
admin@llit.kr [2](*Corresponding Author*)
Dept. of Cyber Security,
Kyungil University Kyungsan,
Kyungbuk 712-701, Korea
kim@kiu.ac.kr

Abstract

Password-based authenticated key agreement is widely used for systems that control remote access to computer networks. It has dual purposes of authentication and key agreement between two parties. Recently, Wang et al. were provided cryptanalysis focused on some attacks, especially for the password guessing attack, from a previous password-based authentication scheme and proposed a robust scheme to cope with the attacks. However, this paper points out that Wang et al.'s scheme has high computational overhead and proposes an anonymous password-based authenticated key agreement scheme with non-tamper resistant smart cards to reduce the overhead. The proposed scheme meets all the criteria required for the authenticated key agreement scheme and eliminates security threats.

Keywords*: Network Security, Cryptanalysis, Authentication, Key Agreement, User Anonymity, Smart Card*

1. Introduction

Many systems that control remote access to computer networks use password-based authentication and many people researched about how to make secure authentication. Since Chang and Wu first presented remote user authentication scheme using smart cards in 1993, there have been many smartcard based authentication schemes [1-3]. Most of previous authentication schemes assumed that the smartcard is tamper-resistant [4-7]. So the remote user authentication schemes using smart cards are not provided against if smart card is easy to forge due to the researches in [8-9]. So the scheme can be vulnerable to various attacks like user impersonation attacks, server masquerading attacks, and offline password guessing attacks, and so on, if the password-based remote user authentication scheme is based on tamper resistant smart cards.

In DBSec'11, Li *et al*. showed that Kim and Chung's password-based remote user authentication scheme in [10] is vulnerable to various attacks if the smart card is non-tamper resistant and they also proposed the improved version, which claimed that their scheme is secure against smart card security breach attacks [11].

*is the corresponding author.

ISSN: 1738-9976 IJSIA

However, Wang *et al*. presented that Li *et al*.'s scheme still cannot withstand offline password guessing attack under the assumption [12]. In addition, Wang *et al*. showed that Li *et al*.'s scheme is also vulnerable to denial of service attack and fails to provide user anonymity and forward secrecy.

Li *et al*.'s scheme in [11] is based on hash and XOR operations, which requires low computational overhead, but is failed to provide security in some attacks. Thereby, Wang *et al*. tried to solve the security problems in Li *et al*.'s scheme by adopting modular exponentiation and public-key cryptography properties, which requires about more than 10 times overhead than hash operation. It looks like that their scheme is successful in the concept of security but requires too much operation overhead even if a session key should be derived by using modular exponentiation to support the forward secrecy.

Thereby, the purpose of this paper is to devise an operation efficient anonymous password-based authenticated key agreement scheme with non-tamper resistant smart cards to solve the overhead problem in Wang *et al*.'s scheme and security problems in Li *et al*.'s schemes, respectively. The proposed scheme could combine advantages from both schemes, which could provide user anonymity, mutual authentication, and forward secrecy and could secure against various attacks including offline password guessing attack even with the assumption that the smart card is non-tamper resistant, impersonation attacks, replay attack, and so on.

The remainder of this paper is organized as follows: in Section 2, we explain the configuration that proposed scheme used and required security criteria. Our proposed scheme is presented in Section 3, and its security analysis and performance analysis are given in Section 4. Section 5 concludes the paper.

2. Background

This section provide network configuration for the proposed authenticated key agreement scheme and set the security goals by providing required security criteria of the scheme.

2.1. Network Configuration

The network configuration of the authenticated key agreement scheme, which is target of this paper, is shown in Figure 1. There are three main participants in the network, which are a user, a client with smart card, and a server. It is assumed that the user should issue his (or her) smart card from the server. The client has to get the possibility access to the smart card of the user and needs to communicate with the remote server via Internet, which is unsecure. Furthermore, it is assumed that all the computations related with the security are performed in the smart card.

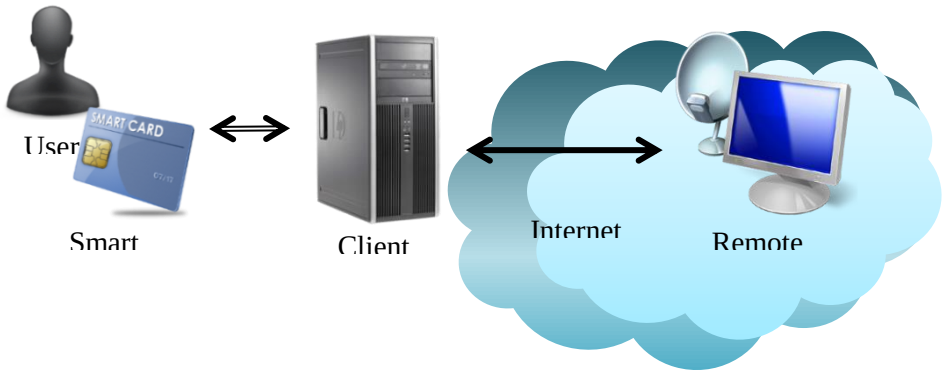

Figure 1. Network Configuration

2.2. Required Security Criteria

This subsection reviews the required security criteria to set our security goals to devise a new authenticated key agreement scheme by summarizing the research efforts from [2, 3, 13-15]. The following criteria are important for smart card based remote user authentication schemes in terms of friendliness, security and efficiency: (C1) the server needs not to maintain a security-sensitive verification table; (C2) the password is memorable, and can be chosen freely by the user; (C3) the password cannot be derived by the privileged administrator of the server; (C4) the security of the scheme is not based on the tamper resistance assumption of the smart card; (C5) the scheme can resist various kinds of sophisticated attacks, such as offline password guessing attack, replay attack, parallel session attack, denial of service attack, stolen verifier attack, user/server impersonation attack; (C6) the password cannot be broken by guessing attack even if the smart card is lost/stolen and compromised; (C7) the client and the server can establish a common session key during the authentication process; (C8) the scheme is not prone to the problems of clock synchronization and time-delay; (C9) the user can change the password locally without any interaction with the authentication server; (C10) the scheme can achieve mutual authentication; (C11) the scheme preserves user anonymity to avoid partial information leakage; (C12) the scheme provides the property of forward secrecy, which is very important when making security feature for authentication schemes with session keys establishment as mentioned in [15].

3. Proposed Authenticated Key Agreement Scheme

As mentioned previously, Wang *et al.*'s scheme has a big operational overhead, which requires many exponentiations. To reduce the overhead, this section proposes a new anonymous password based authenticated key agreement scheme with non-tamper resistant smart cards. The proposed scheme is consisted of three phases, which are registration phase, login and verification phase and password change phase. Notations used in this paper are summarized in Table 1.

3.1. Registration Phase

Let x denote the server S's private key and $Y=g^x \bmod n$ denote its corresponding public key, where x is kept secret by S and Y is stored inside each user's smart card. The registration phase involves the following operations:

Step R1. U_i chooses his (or her) identity ID_i and password PW_i, generates a random number b, and computes $h(b \| PW_i)$. $U_i \Rightarrow S$: $\{ID_i, h(b \| PW_i)\}$.

Step R2. On receiving the message, S checks the validity of ID_i. Only if the validation is successful, S computes $C_1=h(h(ID_i) \oplus x)$, $C_2=C_1 \oplus h(b \| PW_i) \oplus h(ID_i)$, $C_3=h(C_1)$, and $C_4=h(b \| PW_i) \oplus h(x \| Y)$. $S \Rightarrow U_i$: A smart card, SC, containing security parameters $\{C_2, C_3, C_4, h(\cdot), n, g, Y\}$.

Step R3. Upon receiving SC, U_i computes $B=b \oplus ID_i \oplus PW_i$ and enters it into his (or her) SC.

3.2. Login and Verification Phase

When U_i wants to login the system, the following operations will be performed:

Table 1. Notations

Symbol	Description
U_i	The i^{th} user
S	The remote server
ID_i	The identity of user U_i
PW_i	The password of user U_i
SC	The U_i's smart card
x	The private key of S
Y	The public key of S
n	A large prime number
g	A primitive element in Galois Field, $GF(n)$
b, v, w	The random numbers
SK	The session key between U_i and S
$h(\cdot)$	The collision free one-way hash function
$\oplus$	The bitwise XOR operation
$\|$	The string concatenation operation
$A \rightarrow B : C$	Message C is transferred through a common channel from A to B
$A \Rightarrow B : C$	Message C is transferred through a secure channel from A to B

Step L1. U_i inserts his (or her) SC into the card reader and inputs ID_i^* and PW_i^*. SC computes $b^*=B \oplus ID_i \oplus PW_i$, $C_1^*=C_2 \oplus h(b^* \| PW_i^*) \oplus h(ID_i^*)$ and $C_3^*=h(C_1^*)$ and verifies the validity of C_3^* by checking whether C_3^* equals to the stored C_3. If the verification holds, it implies the authenticity of U_i. Otherwise, the session is terminated. SC chooses a random number v and computes $V=g^v \bmod n$, $h(x \| Y)=C_4 \oplus h(b^* \| PW_i)$, $CID_i=h(ID_i) \oplus h(V \| h(x \| Y))$ and $M_1=h(CID_i \| V \| C_1)$. After that, $SC \rightarrow S : \{CID_i, V, M_1\}$.

Step L2. On receiving the login message, S computes $h(x \| Y)$ and $C_1^*=h(h(ID_i) \oplus x)$, and checks the validity of M_1 by comparing it with the computation of $h(CID_i \| V \| C_1^*)$. If they are the same, S chooses a random number w and computes $W=g^w \bmod n$, $SK=V^w \bmod n$ and $M_2=h(SK \| W \| C_1^*)$. After that, $S \rightarrow SC : \{M_2, W\}$.

Step L3. On receiving the message, SC computes $SK^*=W^v \bmod n$ and compares M_2 with the computation of $h(SK^* \| W \| C_1)$. If they are not equal, the session is terminated. Otherwise, SC computes $M_3=h(M_2 \| C_1 \| SK^*)$. After that, $SC \rightarrow S : \{M_3\}$.

Step L4. After receiving the message, S checks if M_3 is equal to the computed value of $h(M_2 \| C_1 \| SK)$. If this verification holds, S authenticates U_i and the login request is accepted. Otherwise, the connection is terminated.

U_i and S agree on the common session key SK for securing future data communications.

3.3. Password Change Phase

In this phase, we argue that the user's SC must have the ability to detect the login failure trials. Once the number of login failure exceeds a predefined system value, the SC must be locked immediately to prevent the exhaustive password guessing behavior. This phase involves the following steps.

Step P1. U_i inserts his (or her) SC into the card reader and inputs ID_i^* and PW_i^* and a new password, PW_i^{new}. SC computes $b^*=B \oplus ID_i \oplus PW_i$, $C_1^*=C_2 \oplus h(b^* \| PW_i^*) \oplus h(ID_i^*)$ and $C_3^*=h(C_1^*)$ and verifies the validity of C_3^* by checking whether C_3^* equals to the stored C_3. If the verification

holds, it implies the authenticity of U_i. Otherwise, the password change request is rejected. *SC* computes $B^{new}=b \oplus ID_i \oplus PW_i^{new}$, $C_2^{new}=C_1^{*} \oplus h(b \| PW_i^{new}) \oplus h(ID_i^{*})$ and $C_4^{new} = C_4 \oplus h(b \| PW_i^{*}) \oplus h(b \| PW_i^{new})$. Thereafter, *SC* substitutes B^{new}, C_2^{new} and C_4^{new} into B, C_2 and C_4 stored in *SC*, respectively.

4. Analysis

This section provides security analysis and performance analysis. Security analysis is focused on the security criteria as mentioned in Section 2. Performance analysis will be focused on the operational overhead by providing comparisons with the related schemes [5, 11, 12, 16].

4.1. Security Analysis

Although it is important to provide a formal security proof on any cryptographic schemes, most published user authentication schemes using smart cards have been demonstrated with a simple proof due to the formal security proof of user authentication schemes remains one of the most challenging issues for cryptography research [17].

The security of the proposed authentication scheme is based on the secure hash function and the discrete logarithm problem. This section will provide security analysis of the proposed scheme focused on the security requirements mentioned in Section 2 under the assumption that the secret information stored in the smart card can be revealed, *i.e.*, the security parameters $\{C_2, C_3, C_4, h(\cdot), n, g, Y, B\}$ can be obtained by a malicious privileged user.

(1) User Anonymity

Suppose that an attacker has intercepted U_i's authentication messages $\{CID_i, V, M_1\}$, $\{M_2, W\}$ and $\{M_3\}$. After that, the adversary may try to retrieve any static parameter from these messages, but these messages are all session-variant and indeed random strings due to the randomness of v or w. Accordingly, without knowing the random numbers, the attacker will face to solve the discrete logarithm problem to retrieve the correct value of ID_i from CID_i, while ID_i is the only static element corresponding to U_i in the transmitted messages. Hence, the proposed scheme can preserve user anonymity.

(2) Offline Password Guessing Attack

Suppose that a malicious privileged user U_i has got a legal user U_k's smart card *SC*, and the secret information $\{B, C_2, C_3, C_4, h(\cdot), n, g, Y\}$ can also be revealed under the assumption of the non-tamper resistant smart card. Even after gathering this information, the attacker has to guess at least both of ID_k and PW_k correctly at the same time, because it has been demonstrated that the proposed scheme can provide identity protection. It is impossible to guess these two parameters correctly at the same time in polynomial time. Furthermore, the attacker needs to know b from B but it is also impossible to know due to the lack of knowledge on both of ID_k and PW_k. Thereby, the proposed scheme can resist against offline password guessing attack with smart card security breach.

(3) Stolen Verifier Attack and Password Disclosure to Server

In the proposed scheme, no sensitive verifiers corresponding to users are maintained by *S*. Therefore, the proposed scheme is free from the stolen verifier

attack. With $h(b \| PW_i)$ instead of plaintext password PW_i submitted to S, it is computationally infeasible to derive PW_i from $h(b \| PW_i)$ without knowing the random number b due to the one-way property of the secure hash function.

(4) User Impersonation Attack

As CID_i, C_2, C_3, C_4, M_1, M_2 and M_3 are all protected by secure one-way hash function, any modification to these parameters of the legitimate U_i's authentication messages will be detected by S if the attacker cannot fabricate the valid CID_i^*. Because the attacker has no way of obtaining the values of ID_i, PW_i and $h(x \| Y)$ corresponding to U_i, he (or she) cannot fabricate the valid CID_i^*, M_1, M_2 and M_3. Therefore, the proposed scheme is secure against user impersonation attack.

(5) Server Masquerading Attack

In the proposed scheme, a malicious server MS cannot compute the correct $M_2= h(SK \| W \| C_1^*)$ because he (or she) does not know S's private key x. Thereby, MS cannot compute or know C_1^*, and thus cannot derive the valid ID_i. Without knowing U_i's valid ID_i and S's private key x, MS has to break the secure one-way hash function to retrieve $h(ID_i)$. Furthermore, because MS cannot obtain $h(ID_i)$, it is impossible to fabricate the proper $C_1^*=h(h(ID_i)\oplus x)$ to pass the verification of U_i in Step L2 of the verification phase. Therefore, the proposed scheme is secure against server masquerading attack.

(6) Replay Attack and Parallel Session Attack

The proposed scheme can withstand from the replay attack because the authenticity of the messages $\{CID_i, V, M_1\}$, $\{M_2, W\}$ and $\{M_3\}$ are verified by checking the fresh random number v and/or w. On the other hand, the proposed scheme resists from the parallel session attack, in which an attacker may masquerade as legitimate user U_i by replaying a previously intercepted authentication message from the other legal user. The attacker cannot compute valid C_1^* because he (or she) does not know the value of $h(ID_i)$ corresponding to U_i. Therefore, the resistance to replay attack and parallel session attack can be guaranteed in the proposed scheme.

(7) Mutual Authentication

In the proposed scheme, S authenticates U_i by checking the validity of M_3 in the access request. We have shown that the proposed scheme can preserve user anonymity, so U_i's identity ID_i is even secured to the server S but only exposed $h(ID_i)$ to S. We have proved that the proposed scheme can resist user impersonation attack. Therefore, it is impossible for an adversary to forge messages to masquerade as U_i in the proposed scheme. To pass the authentication of S, the smart card first needs to take U_i's identity ID_i and password PW_i to get through the verification in Step L2 of the login phase. In this Section, we have shown that the proposed scheme can resist offline password guessing attack. Therefore, only the legal user U_i who owns correct ID_i and PW_i can pass the authentication of S. On the other hand, U_i authenticates S by explicitly checking whether the other party communicating with can compute the valid M_2 or not. Since MS does not know the values of ID_i corresponding to U_i and x corresponding to S, only the legitimate S could compute the correct $M_2=h(SK \| W \| C_1)$. From the above analysis, we conclude that the proposed scheme can achieve mutual authentication.

(8) Denial of Service Attack

Assume that an attacker has got a legitimate U_i's smart card. However, in the proposed scheme, the smart card computes $C_3^*=h(C_2 \oplus h(b^* \| PW_i^*) \oplus h(ID_i^*))$ and compares it with the stored C_3 in its memory to checks the validity of U_i's identity ID_i and password PW_i before the password update procedure. It is not possible for the attacker to guess out U_i's s identity ID_i and password PW_i correctly at the same time in polynomial time. Moreover, once the number of login failure exceeds a predefined system value, the smart card will be locked immediately. Therefore, the proposed scheme is secure against denial of service attack.

(9) Forward Secrecy

Following the proposed scheme, U_i and S can establish the same session key $SK=V^w \bmod n=W^v \bmod n=g^{vw} \bmod n$. Based on the difficulty of the computational Diffie-Hellman problem, any previously generated session keys cannot be revealed without knowledge of the ephemeral v and w. As a result, the proposed scheme provides the property of forward secrecy.

4.2. Performance Analysis

To evaluate the proposed scheme, this section provides two comparisons for the performance and the satisfaction of the criteria among relevant authentication schemes. Since there are only some schemes that can withstand from the offline password guessing attack under the non-tamper resistance assumption of the smart cards, the schemes in [5, 16, 18] are chosen for the comparisons. The comparison results are depicted in Tables 2 and 3, respectively.

Table 2. Performance Comparison between Schemes

	Proposed scheme	Wang *et al.* [12]	Li *et al.* [11]	Chen *et al.* [5]	Horng *et al.* [16]
TC	$4T_E+13T_H$	$6T_E+12T_H$	$12T_H$	$6T_E+5T_H$	$7T_E+4T_S+8T_H$
COM	2560 bits	2560 bits	856 bits	2560 bits	2432 bits
SO	4480 bits	3456 bits	384 bits	3200 bits	3328 bits

Since the login phase and verification phase are executed much more frequently than the other two phases, only the computation cost, communication overhead and storage cost of the login phase and verification phase are taken into consideration. Without loss of generality, ID_i and PW_i, random numbers, timestamp values and output of one-way hash function are all recommended to be 128-bit long, while n, y and g are all 1024-bit long. Let T_H, T_E, T_I, T_S and T_X denote the time complexity for hash function, exponential operation, inverse operation, symmetric cryptographic operation and XOR operation, respectively. Since the time complexity of XOR operation is negligible as compared to the other three operations, we do not take T_X into account. Typically, time complexity (TC) associated with these operations can be roughly expressed as $T_E \approx T_I > T_S \geq T_H \gg T_X$ [19–21]. In the proposed scheme, the parameters $\{C_2, C_3, C_4, n, g, Y, B\}$ are stored in the smart card, thus the storage overhead (SO) is 4480(=3×128+4×1024) bits. The communication overhead (COM) includes the capacity of transmitting message involved in the login and verification phase, which is 2560(=4×128+2×1024) bits. During the login and verification phase, the total computation cost of U_i and S is $4T_E + 13T_H$. As shown in Table 2, the proposed scheme is more efficient than the other schemes except Li *et al.*'s scheme.

Table 3. Security Comparison between Schemes

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wang *et al*.[12]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Li *et al*.[11]	No	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	No	No
Chen *et al*.[5]	Yes	Yes	No	Yes	No	No	Yes	No	No	Yes	No	No
Horng *et al*.[16]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes

As compared to Li *et al*.'s scheme, to withstand offline password guessing attack, public-key techniques are employed [22], and thus at least two exponentiations are required; to provide the feature of forward secrecy, the generation of the session key based on the Diffie-Hellman key exchange algorithm is common. To conquer all the identified security flaws, the decrease of some performance is unavoidable and reasonable.

Table 3 gives a comparison based on the required security criteria between authentication schemes. It is clear that the proposed scheme and Wang *et al*.'s scheme meet more criteria as compared to the other relevant authentication schemes using non-tamper resistant smart cards.

5. Conclusion

This paper had been proposed an operation efficient anonymous password-based authenticated key agreement scheme with non-tamper resistant smart cards to solve the overhead problem in Wang *et al*.'s scheme and security problems in the related authentication schemes, respectively. The proposed scheme could combine advantages from both schemes, which could provide user anonymity, mutual authentication, and forward secrecy and could secure against various attacks including offline password guessing attack even with the assumption that the smart card is non-tamper resistant, impersonation attacks, replay attack, and so on. It could be used to the various network environments as a basic secure building block. In future work, we will develop a practical formal method for security analysis of authentication schemes using smart cards.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] C. C. Chang, T. C. Wu, "Remote password authentication with smart cards," IEE Proceedings-E, vol. 138, no. 3, **(1993)**, pp. 165-168.
[2] I. E. Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over insecure networks," Journal of Computer and System Sciences, vol. 72, no. 4, **(2006)**, pp. 727–740.
[3] S. K. Sood, "Secure Dynamic Identity-Based Authentication Scheme Using Smart Cards," Information Security Journal, vol. 20, no. 2, **(2011)**, pp. 67–77.
[4] H. S. Kim, S. W. Lee, K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, **(2003)**, pp. 32-41.
[5] Y. Chen, J. S. Chou, C. H. Huang, "Improvements on two password-based authentication protocols," Cryptology ePrint Archive, Report 2009/561, **(2009)**.
[6] J. Xu, W. T. Zhu, D. G. Feng, "An improved smart card based password authentication scheme with provably security," Computer Standards & Interface, vol. 31, no. 4, **(2009)**, pp. 723-728.
[7] S. K. Sood, "Secure Dynamic Identity-based Authentication Scheme using Smart cards," Information Security Journal, vol. 20, no. 2, **(2011)**, pp. 67-77.

[8] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis," Lecture Notes in Computer Science, vol. 1666, **(1999)**, pp. 388-397.
[9] F. X. Standaert, T. G. Malkin, M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," Lecture Notes in Computer Science, vol. 5479, **(2009)**, pp. 443-461.
[10] S. K. Kim, M. G. Chung, "More secure remote user authentication scheme," Computer Communications, vol. 32, no. 6, **(2009)**, pp. 1018-1021.
[11] C. T. Li, C. C. Lee, C. J. Liu, C. W. Lee, "A Robust Remote User Authentication Scheme against Smart Card Security Breach," Lecture Notes in Computer Science, vol. 6818, **(2011)**, pp. 231-238.
[12] D. Wang, C. G. Ma, P. Wu, "Secure Password-based Remote User Authentication Scheme with Non-tamper Resistant Smart Cards," Lecture Notes in Computer Science, vol. 7371, **(2012)**, pp. 114-121.
[13] R. C. Wang, Juang, W. S., C. L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," Computer Communications, vol. 34, no. 3, **(2011)**, pp. 274–280.
[14] S. H. Wu, Y. F. Zhu, Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," Security and Communication Networks, vol. 5, no. 2, **(2012)**, pp. 236–248.
[15] S. B. Wilson, D. Johnson, A. Menezes, "Key agreement protocols and their security analysis," Lecture Notes in Computer Science, vol. 1355, **(1997)**, pp. 30–45.
[16] W. B. Horng, C. P. Lee, J. Peng, "A secure remote authentication scheme preserving user anonymity with non-tamper resistant smart cards," WSEAS Transactions on Information Science and Applications, vol. 7, no. 5, **(2010)**, pp. 619–628.
[17] D. He, M. Ma, Y. Zhang, C. Chen, "A strong user authentication scheme with smart cards for wireless communications," Computer Communications, vol. 34, no. 3, **(2011)**, pp. 367–374.
[18] H. R. Chung, W. C. Ku, M. J. Tsaur, "Weaknesses and improvement of Wang *et al.*'s remote user password authentication scheme for resource-limited environments," Computer Standards & Interfaces, vol. 31, no. 4, **(2009)**, pp. 863–868.
[19] W. B. Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, New Jersey, **(2004)**.
[20] D. S. Wong, H. H. Fuentes, A. H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices," Proceedings of ACSAC'01, **(2001)**, pp. 92–101.
[21] N. R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," IEEE Transactions on Mobile Computing, vol. 5, no. 2, **(2006)**, pp. 128–143.
[22] S. Halevi, H. Krawczyk, "Public-key cryptography and password protocols," ACM Transactions on Information and System Security, vol. 2, no. 3, **(1999)**, pp. 230–268.

Authors

Yunghee Lee, he is a student at the Department of Cyber Security, Kyungil University, Korea from 2012. He has been attended Information Security Laboratory supervised by Prof. Hyunsung Kim from 2012 and as a researcher at Research Institute of Information Cross-over Security at Kyungil University, respectively. His research interests include smartphone security, uHealthcare security, cloud computing security, digital forensics, information security, network security and ubiquitous computing security.

Hyunsung Kim, he is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.