NFC Based Privacy Preserving User Authentication Scheme in Mobile Office

Jungsub Ahn[1], Sung Woon Lee[2], Hyunsung Kim[3]*

[1] The Department of Computer Engineering, Kyungil University, Kyungsan, Kyungbuk, Korea.
[2] The Department of Information Security, Tongmyong University, Korea.
[3] The Department of Cyber Security, Kyungil University, Korea.

* Corresponding author. Tel.: +82 53-600-5621; email: kim@kiu.ac.kr
Manuscript submitted October 2, 2014; accepted May 3, 2015.
doi: 10.17706/ijcce.2016.5.1.61-70

Abstract: Smartwork is a flexible type of work that provides users with a more convenient work possibility, which refers to employees who work away from the company's office in any capacity. Smartwork technologies often need additional protection because their nature generally places them at higher exposure to external threats. Therefore, smartwork application should provide securing infrastructures for both of users, inside and outside of the organization. This paper proposes a NFC based privacy preserving user authentication scheme as a basic security building block for smartwork environment, which is focused only on the mobile office one of smartwork environment. The proposed scheme provides anonymity and untraceability, which requires for the ubiquitous environment applications. The proposed scheme could be used as a basic building block for security on the various smartwork environments.

Key words: Smartwork, NFC, authentication, privacy, security, mobile office.

1. Introduction

As smartwork initiatives expand in scope and spread from the public to private sectors, more workers in Korea are embracing flexible work and lifestyle patterns [1]-[4]. Smartwork systems are designed to optimize productivity and efficiency by providing remote access to work materials and operating systems, allowing workers to work at home or in specially constructed centers. Video and telephone conferencing eliminate the need for travel and save the time spent attending meetings and making face-to-face reports. Along with desktops and laptop computers, mobile devices such as smartphones and tablet personal computers also connect to smartwork systems to enable work on-the-go.

Smartwork has been thought to satisfy both employees and a company's interests, which are usually contradictory. Nonetheless, there are critical barriers of introducing smartwork because of security issues. Proper introduction of smartwork requires a security protection model which allows efficient management of threats and vulnerabilities [5]-[8]. These can be accomplished through a combination of security features built into the remote access solutions and additional security controls applied to the smartwork devices.

There are only little security related researches on smartwork [5], [6], [9], [10]. Choi *et al.* derived threats through structured interview with heavy users or designers of smartwork and verified the derived threats by survey [5]. Byun *et al.* proposed the security management architecture for the construction of a secure smartwork center [6]. The security management architecture is only conceptual model but does not provide the detailed steps for the security mechanism. Won proposed a secure user authentication method using

NFC in smartwork environment, which provides the detailed steps for authentication [9]. Won argued that the authentication method is secure, which prevents from unauthorized users by generating session key using random key and comparing. Kim in [10] provided analyses on the environment and security issues on smartwork and near field communication (NFC) environment. After that he defined privacy issues to build the NFC-based security system and investigate requirements to set up the security system. Kim's research has good point on issuing privacy issues in smartwork environment but that also provide the direction of security research.

In this paper, we propose a new NFC based privacy preserving user authentication scheme in mobile office to realize Kim's proposal for smartwork environment security and privacy. The proposed scheme provides anonymity and untraceability, which requires for the ubiquitous environment applications. The proposed scheme could be used as a basic building block for security on the various smartwork environments.

2. Related Work

This section reviews security schemes, which will be used in the proposed scheme and smartwork environment, which is required to understand this paper.

2.1. Security Schemes

This subsection describes security schemes used in the proposed scheme as the basic security building blocks, which are Diffie-Hellman key exchange mechanism, cryptographic hash function and symmetric-key cryptosystem.

Diffie-Hellman key exchange mechanism: Diffie–Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network [11]. The simplest and the original implementation of the protocol use the multiplicative group of integers modulo p, where p is a prime and a primitive root modulo p. Here is an example of the protocol, with non-secret values p, g, A and B, and secret values a, b and s.

(DH1) User U_1 chooses a random and secret integer a, computes A as in (1), and sends A to user U_2.

$$A = g^a \bmod p \tag{1}$$

(DH2) User U_2 chooses a random and secret integer b, computes B as in (2), and sends B to user U_1.

$$B = g^b \bmod p \tag{2}$$

(DH3) U_1 computes s as in (3) and U_2 computes s as in (4). U_1 and U_2 now share a secret s.

$$s = B^a \bmod p \tag{3}$$

$$s = A^b \bmod p \tag{4}$$

Both U_1 and U_2 have arrived at the same value, because $(g^a)^b$ and $(g^b)^a$ are equal over mod p. Note that only a, b, and ($g^{ab} \bmod p = g^{ba} \bmod p$)are kept secret. All the other values – p, g, $g^a \bmod p$, and $g^b \bmod p$ – are sent in the clear.

Cryptographic hash function: A cryptographic hash function is a hash function, which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone [12]. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

The ideal cryptographic hash function has four main properties: it is easy to compute the hash value for any given message, it is infeasible to generate a message that has a given hash, it is infeasible to modify a message without changing the hash and it is infeasible to find two different messages with the same hash. Cryptographic hash functions have many information security applications, but we will only consider the message authentication codes and forms of authentication of message. The secure hash algorithm (SHA) is a family of cryptographic hash functions published by the national institute of standards and technology (NIST) [13]. We will consider the usage of SHA in this paper.

Symmetric-key cryptosystem: Symmetric-key cryptosystem is a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext [14]. The keys may be identical or there may be a simple transformation to go between the two keys. The keys represent a shared secret between two or more parties that can be used to maintain the private information. The advanced encryption standard (AES) is a specification for the symmetric-key cryptosystem by NIST in 2001 [15]. For AES, NIST selected usages of three different key lengths, 128, 192 and 256 bits, each with a block size of 128 bits. We consider AES 128 bits as a symmetric-key cryptosystem in our scheme.

2.2. Smartwork Environment

To support smartwork, Korea Communications Commission (KCC) categorizes three ways of smartwork including home office, mobile office and smartwork center as shown in Fig. 1.

Mobile office is a new type of working method in the workplace that can be used at any time or anywhere by connecting to the network with mobile devices. It is consisted with a mobile device, authentication server, and a database (DB) server. A mobile device works as a client device, which could be smart phone, table personal computer, and any other similar hand held devices. The device could accompany with NFC to keep secret information and to communicate with other devices. The mobile device could communicate with the smartwork server via wireless network like 3G, 4G, WiBro or WiFi. Authentication server at smartwork server side registers the employee and performs the login for them, which could also work as a registration center. The mobile device could access the smartwork server via the authentication server.

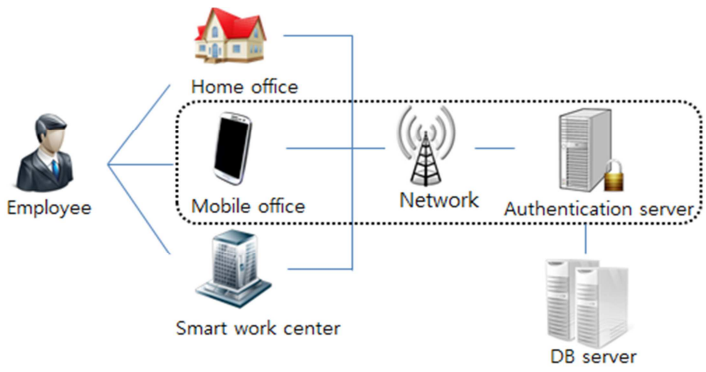

Fig. 1. Conceptual model for smartwork environment.

Recently, there are many companies to support smartwork by using mobile office via smart phone allowing workers to work at home or in specially constructed centers for the work efficiency and to reduce budget. Currently, it is tendency to expand the range of coverage by using mobile office from e-mail and instant messenger usage to the business support, which is very specialized business areas focused on a specific industry [16]. However, security should be solved to support an expanded business for smartwork environment to cope from various attacks.

NFC is a high frequency wireless short distance communication standard defined in the ISO/IEC 18092 standard [17]. There are three different operating modes, read/write mode, peer to peer mode and card

emulation mode, according to the specification. We will only consider the card emulation mode in this paper. It is also assumed that a worker has NFC and a smart device and a company has a smartwork server with an authentication server as shown in Fig. 2.

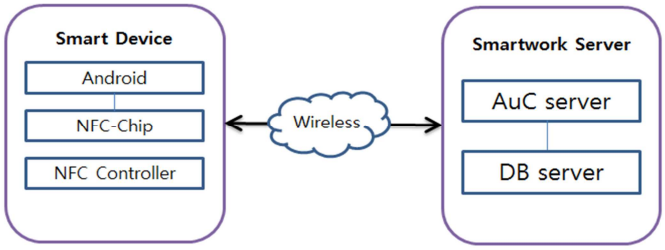

Fig. 2. Mobile office configuration.

3. Proposed Authentication Scheme

This section proposes a privacy preserving user authentication scheme (PAS) using NFC for smartwork environment. The PAS shown in Fig. 3 is divided into four phases: user registration phase, mobile registration phase, user authentication phase and password updating phase. Table 1 shows notations used in this paper.

Table 1. Notations

Notation	Description
ID_i	Identity of an worker
U_i	Employee i
CID_i	Dynamic identity
PW_i	Password of U_i
DPW_i	Amplified password of U_i
s	Master secret key of a server
g	Group generator over Z_p
PU_s	Public key of a server
SK	Session key
$IMEI_i$	Device identification of U_i
$DIMEI_i$	Amplified device identification of U_i
$CIMEI_i$	Dynamic device identification of U_i
AMK	Device authentication key
a, b, r, d, rn	Random numbers
MAC	Message authentication code
$H()$	Cryptographic hash function using SHA-256
$E()$	Symmetric key cryptosystem using AES
$\|\|$	Concatenation operation
$\oplus$	Exclusive-OR operation

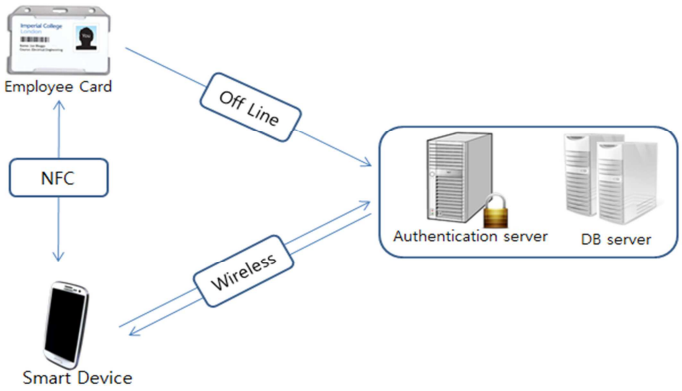

Fig. 3. Overview of the proposed authentication scheme.

3.1. User Registration

When a worker U_i wants to be registered to the server, he (or she) chooses a random number r, inputs ID_i and PW_i, computes DPW_i as in (5), and sends ID_i and DPW_i to the smartwork server via off-line. The smartwork server performs the following operations

$$DPW_i = H(PW_i||r) \tag{5}$$

(UR1) Computes Y as in (6) and APK as in (7), where s is the server's secret key.

$$Y = H(ID_i||s) \tag{6}$$

$$APK = H(DPW_i \oplus \mathrm{Y}) \tag{7}$$

(UR2) Issues an IC card to U_i, which stores Y, $E()$, $H()$, PU_S and APK, where PU_S in (8) is the server's public key. It is note that the issued IC card has NFC functionality.

$$PU_s = g^{\mathrm{s}} \bmod p \tag{8}$$

After this, U_i puts r on the card.

3.2. Mobile Device Registration

A user installs a smartwork application on his (or her) mobile device after downloading it from the smartwork server. U_i asks a mobile device registration by inserting his NFC to the NFC reader and by asking $IMEI_i$ from the mobile device. Overall processes for the mobile device registration are as follows

(MR1) U_i inputs ID_i, PW_i and $IMEI_i$ to the NFC.

(MR2) The NFC chooses a random number d and computes $DIMEI_i$ as in (9). After that, it derives APK after computing DPW_i by using the inputted PW_i and the stored R_{UR}. The NFC generates a new random number a, computes R_A as in (10), V_A as in (11), USS as in (12), M_{DR} as in (13), CID_i as in (14) and MAC_{DR} as in (15) and sends a mobile device request message$\{CID_i, R_A, M_{DR}, MAC_{DR}\}$ to the smartwork server.

$$DIMEI_i = H(IMEI_i||d) \tag{9}$$

$$R_A = g^a \bmod p \tag{10}$$

$$V_A = (PU_s)^{\mathrm{a}} \bmod p \tag{11}$$

$$USS = H(Y) \tag{12}$$

$$M_{DR} = E_{USS}(DIMEI_i) \tag{13}$$

$$CID_i = ID_i \oplus H(R_A||V_A) \tag{14}$$

$$MAC_{DR} = H(CID_i||USS||R_A||M_{DR}) \tag{15}$$

(MR3) When the smartwork server receives the message, it verifies the message by checking MAC_{DR}. The integrity check is performed by computing V_A' as in (16), ID_i' as in (17), USS' as in (18) and MAC_{DR}' as in (19). Only if MAC_{DR} is the same as the computed MAC_{DR}', it decrypts M_{DR}, computes AMK as in (20), M_{RM} as in (21),

MAC_{RM} as in (22) and sends a response message $\{M_{RM}, MAC_{RM}\}$ to the NFC.

$$V_A' = (R_A)^s \bmod p \tag{16}$$

$$ID_i' = CID_i \oplus H(R_A||V_A') \tag{17}$$

$$USS' = H(H(ID_i'||s)) \tag{18}$$

$$MAC_{DR}' = H(CID_i||USS'||R_A||M_{DR}) \tag{19}$$

$$AMK = H(DIMEI_i||s) \tag{20}$$

$$M_{RM} = E_{USS}(AMK) \tag{21}$$

$$MAC_{RM} = H(USS'||M_{RM}) \tag{22}$$

(MR4) After receiving the message, the NFC sends AMK and d to the mobile device only if the integrity check of MAC_{RM} is successful. The mobile device keeps them in secret.

3.3. User Authentication

An employee U_i uses the smartwork application on his (or her) mobile device to ask a service access by inputting and sending ID_i and PW_i to the NFC. The mobile device sends $DIMEI_i$ and AMK to the NFC. Overall processes for the user authentication as shown in Fig. 4 are as follows:

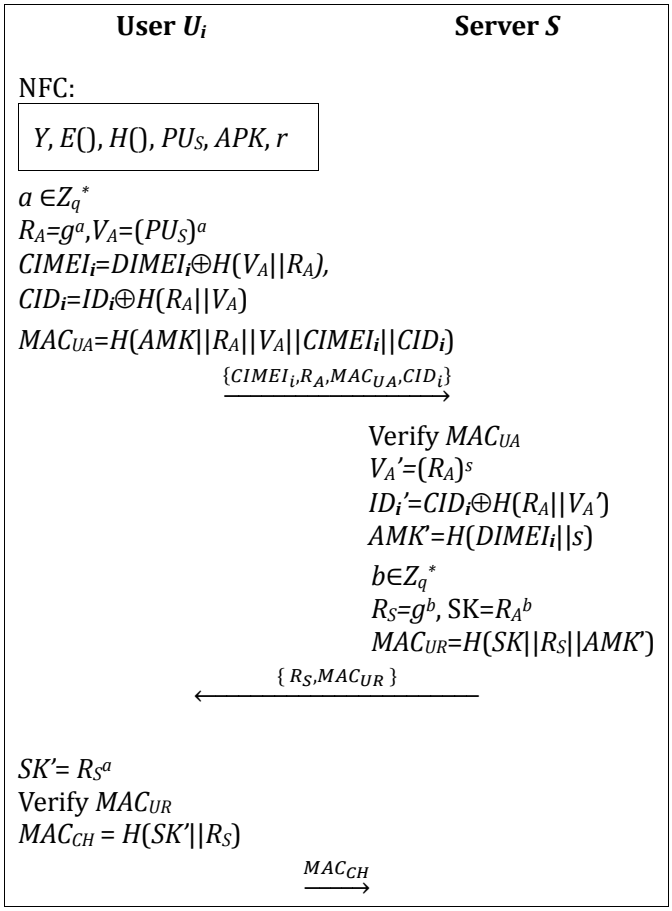

Fig. 4. The proposed authentication scheme.

(UA1) The NFC derives APK by computing DPW_i using the inputted PW_i and the stored r. After that, it generate a new random a and computes R_A as in (10), V_A as in (11), $CIMEI_i$ as in (23), CID_i as in (14) and MAC_{UA} as in (24) and sends a mobile device request message $\{CIMEI_i, R_A, MAC_{UA}, CID_i\}$ to the smartwork server.

$$CIMEI_i = DIMEI_i \oplus H(V_A||R_A) \tag{23}$$

$$MAC_{UA} = H(AMK||R_A||V_A||CIMEI_i||\ CID_i) \tag{24}$$

(UA2) The smartwork server checks the integrity of the message by checking MAC_{UA}. The integrity check is performed by using the derived value V_A' as in (16), ID_i' as in (17). Furthermore, it checks the validity of the device with AMK' as in (25). Only if the verification is successful, it generates a random number b, computes R_S as in (26), SK as in (27) and MAC_{UR} as in (28) and sends the authentication response message $\{R_S, MAC_{UR}\}$ to the mobile device.

$$AMK' = H(DIMEI_i||s) \tag{25}$$

$$R_S = g^b \bmod p \tag{26}$$

$$SK = {R_A}^b \bmod p \tag{27}$$

$$MAC_{UR} = H(SK||R_S||AMK') \tag{28}$$

(UA3) The NFC checks the integrity of the message by checking MAC_{UR}. The integrity check is performed by establishing a session key SK' as in (29) and checking whether MAC_{UR} is the same with $H(SK'||R_S||AMK)$. Only if the verification is successful, it computes MAC_{CH} as in (30) and sends it back to the smartwork server.

$$SK' = {R_A}^b \bmod p \tag{29}$$

$$MAC_{CH} = H(SK'||R_S) \tag{30}$$

3.4. Password Updating

When an employee U_i wants to change his/her password, he (or she) could perform his (or her) phase. The NFC performs the password change only if the user authentication is successful as the same as in the steps on the user authentication phase. The steps for the password updating are as follows:

(PU1) U_i inserts his (or her) NFC into the NFC reader and inputs ID_i, old password PW_i and a new password NPW_i to the NFC.

(PU2) The NFC generates a random number r_n, computes DPW_i as in (5) and $DNPW_i$ as in (31) and updates APK as in (32) and r as in (33).

$$DNPW_i = H(NPW_i||r_n) \tag{31}$$

$$APK = APK \oplus DPW_i \oplus DNPW_i \tag{32}$$

$$r = r_n \tag{33}$$

4. Security Analysis

This section shows that the PAS is secure against various attacks. Analyses are focused on the attacks including offline password guessing attack, replay attack, denial of service (DoS) attack, stolen verifier attack and user impersonation attack and the services including session key agreement and mutual authentication.

4.1. Offline Password Guessing Attack

Offline password guessing attack is performed after intercepting password related information from the message transmissions in the PAS and tries to guess the password by offline. However, the PAS does not use any password related information transmission. The password related information is only stored in the NFC. An active attacker could try offline password guessing attack only if the attacker could steal and read the NFC of a worker. However, there is no way to perform this attack in our scheme due to the one way hash function $H()$ used to the password amplification DPW even if the attacker could get and read the NFC.

4.2. Replay Attack

The PAS uses session dependent random numbers a and b to cope with this attack. An attacker could intercept the messages $\{CIMEI_i, R_A, MAC_{UA}, CID_i\}$, $\{R_S, MAC_{UR}\}$ and MAC_{CH} from the user authentication phase. However, there is no way that the attacker could perform replay attack due to the validation check in each step of the phase. So, the PAS is secure against replay attack due to the difficulty of discrete logarithm problem from the Diffie-Hellman key agreement mechanism.

4.3. Denial of Service Attack

DoS attacks aim at denying or degrading a legitimate user's access to a service or network resource, or at bringing down the servers offering such service [18]. The PAS could cope against this attack due to the usage of MAC in each message at the user authentication phase. For this attack, an attacker should have power to modify proper information in each message. However, there is no way the attacker could get secret key related information in our scheme. Thereby, the PAS is safe from DoS attack.

4.4. Stolen Verifier Attack

The smartwork server does not keep any worker related information at the PAS. All of U_i related information are stored on the NFC of the worker due to the security season. Thereby, there is no way the attacker could get any secret information in our scheme.

4.5. User Impersonation Attack

The attacker cannot derive a legal worker's secret information from eavesdropped messages among U_i, the NFC and the smartwork server. Meanwhile, the attacker cannot forge other worker's NFC from known security information of a malicious inside user due to not using verification table at the server side. Furthermore, the usage of key combined with ID_i could protect the attacker from the user impersonation attack even to the legal user.

4.6. Session Key Agreement

In order to protect the communication between the worker and the smartwork server, a session key needs to be negotiated between them in advance. The PAS uses the Diffie-Hellman key agreement mechanism to compute a session key depending on the fresh session random numbers. By securing the exchange of a and b, the U_i and the server can separately compute the common session key SK.

4.7. Mutual Authentication

Based on the user authentication phase, the PAS can provide mutual authentication among the worker U_i and the smartwork server. In UA2 at the user authentication phase, by checking the validity of MAC_{UA}, the smartwork server can verify the legitimacy of U_i due to the usage of *USS*. In UA3, by checking the validity of MAC_{UR}, U_i can verify the legitimacy of the server because only the server could compute a proper *SK*.

5. Conclusion

This paper has been proposed a NFC based privacy preserving user authentication scheme as a basic security building block for smartwork environment, which is focused only on the mobile office one of smartwork environment. Security analysis shows that the proposed scheme is secure against various attacks and provides anonymity and untraceability, which requires for the ubiquitous environment applications. The proposed scheme could be used as a basic building block for security on the various smartwork environments.

Acknowledgment

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2011-0008890) and also was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] (November 23, 2011). Living smarter with smart work. From http://www.korea.net/NewsFocus/Business/view?articleId=90033

[2] Scarfone, K., Hoffman, P., & Souppaya, M. (2009). Guide to enterprise telework and remote access security. *NIST Special Publication*, *80(46)*.

[3] GSA. (2002). Analysis of home-based telework technology barriers. From http://www.gsa.gov/teleworklibrary

[4] Cha, K. J., & Cha, J. S. (2014). The common challenges to the successful implementation of smartwork program. *International Journal of Multimedia and Ubiquitous Engineering*, *9(2)*, 127-132.

[5] Choi, J., Ra, Y. J., Shin, D., & Jung, Y. G. (2012). The characteristics of smartwork security compare to traditional telework. *International Journal of Security and Its Applications*, *6(2)*, 463-467.

[6] Byun, Y. S., & Kwak, J. (2013). Security management architecture for secure smartwork center. *International Journal of Security and Its Applications*, *7(5)*, 315-320.

[7] Paul, I. (2011). Five big security threats for 2011. *PC World*. From http://www.pcworld.com/article/221780/five_big_security_threats_for_2011.html

[8] Godlove, T. (2010). Telework and mobile computing: Security concerns and risks. *The Security Journal*, *30*, 5-11.

[9] Won, D. (2012). A design of secure user authentication method using NFC in smartwork environment. M.S. Thesis, Soongsil University.

[10] Kim, H. (2014). Investigation on NFC-based security system for smartwork. *Journal of Security Engineering*, *11(3)*, 263-272.

[11] Diffie–Hellman key exchange. Wikipedia. Form http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[12] Cryptographic hash function. Wikipedia. Form http://en.wikipedia.org/wiki/Cryptographic_hash_function

[13] Secure hash algorithm. Wikipedia. From http://en.wikipedia.org/wiki/Secure_Hash_Algorithm

[14] Symmetric-key algorithm. Wikipedia. From http://en.wikipedia.org/wiki/Symmetric-key_algorithm

[15] Advanced encryption standard. Wikipedia. From http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[16] Explore IDC. *IDC Global Mobile OS & Apps Survey.*
[17] GSMA. (2007). *Mobile NFC Technical Guidelines*.
[18] Sisalem, D., Kuthan, J., & Ehlert, S., (2006). Denial of service attacks targeting a SIP VoIP infrastructure: Attack scenarios and prevention mechanisms. *IEEE Network*, *20(5)*, 26-31.

Jungsub Ahn is a student at the Department of Computer Engineering, Kyungil University, Republic of Korea since 2010. His research interests include information security, computer network, near field communication, mobile ad-hoc network, vehicular ad-hoc network security, ubiquitous computing, cloud computing, wireless sensor network and computer algorithm.

Sung Woon Lee is a professor at the Department of Information Security, Tongmyong University, Korea. He received the B.S. and M.S. degrees in computer science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in computer engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, Korea, from 1996 to 2000. His research interests include cryptography, network security, and security protocol.

Hyunsung Kim is a professor at the Department of Cyber Security, Kyungil University, Korea. He received his 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 2011 with the Department of Computer Engineering, Kyungil University. He had been a visiting scholar from 2009 to 2010 with the School of Computing, Dublin City University, Ireland. Currently, he is a full professor at the Department of Cyber Security, Kyungil University. His current research interests are cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.