International Journal of Control and Automation
Vol. 7, No. 12 (2014), pp. 301-310
http://dx.doi.org/10.14257/ijca.2014.7.12.28

NFC based User Authentication Method in Smartwork Environment

Hyunsung Kim[1] and Sung Woon Lee[2]

[1]*Dept. of Cyber Security, Kyungil University,*
Kyungsan, Kyungbuk 712-701, Korea
[2]*(Corresponding Author) Dept. of Information Security, Tongmyong University*
Busan 608-711, Korea
kim@kiu.ac.kr

Abstract

With the advances of IT technology, the interest in smartwork is increasing by using various mobile devices through Internet services at anytime and anywhere. The introduction of smartwork to a company provides business efficiency, improves productivity and reduces costs, but security researches are required to solve a variety of security issues in it. For the secure user authentication, Won proposed a user authentication method using NFC in smartwork environment. However, this paper shows that Won's method has some security problems, including weak against stolen verifier attack and replay attack and lack of message integrity, and proposes a new NFC based user authentication mechanism to solve the problems. The proposed mechanism could be used as a security building block in various smartwork environments including telework, mobile office, and so on.

Keywords: *Smartwork, Telework, Mobile office, Security, Authentication*

1. Introduction

Recently, according to the concern of environmental pollution and quality of life, smartwork has been increasing. 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. It uses smart work devices, mobile device, tablet PC, smart phone, iTab, etc., to the workplace. Smartwork site are becoming increasingly popular, and are well equipped with a variety of advanced IT technology and services [1-3].

Smartwork technologies often need additional protection because their nature generally places them at higher exposure to external threats than applications only accessed from inside of the organization [3]. Therefore, smartwork application should provide securing infrastructures for both of users, inside and outside of the organization. The common security objectives at an application involve Confidentiality – ensure that only legal users could read the message, Integrity – ensure detecting any changes from transmitted messages that occur in transit and Availability - ensure that users could access resources whenever needed.

There are only little security related researches on smartwork [4-7]. Cho et al. derived threats through structured interview with heavy users or designers of smartwork and verified the derived threats by survey [4]. Byun and Kwak proposed a security management architecture for the construction of a secure smartwork center [5]. The security management architecture is only conceptual model but does not provide the detailed steps for the security mechanism. Kim in [6] provided analyses on the environment and security issues on smartwork and near field

ISSN: 2005-4297 IJCA

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. Recently, Won proposed a secure user authentication method using NFC in smartwork environment, which provides the detailed steps for authentication [7]. Won argued that the authentication method is secure, which prevents from unauthorized users by generating session key using random key and comparing.

In this paper, we first show that Won's user authentication method has some security flaws, which are weak against stolen verifier attack and replay attack and have lack of message integrity. Furthermore, we will propose a new NFC based user authentication mechanism to solve the problems. The proposed mechanism could be used as a basic building block for security on the various smartwork environments.

This paper is organized as follows. Section 2 reviews the network architecture for smartwork and the overview of NFC operational mode. Won's user authentication mechanism is reviewed and security analyses on it are provided in Section 3. To solve the security flaws, Section 4 proposes a new NFC based user authentication method to satisfy required security criteria. Some analyses for security and conclusion are given in Sections 5 and 6, respectively.

2. Related Works

This section reviews smartwork environment and NFC operation mode, which are required to understand mechanisms described in this paper.

2.1. Smartwork Environment

Korea communications commission (KCC) defines smartwork as a new work concept to work outside the conventional office at anytime and anywhere [8-9]. To support smartwork, KCC categorizes three ways of smartwork including home office, mobile office and smart working center as shown in Figure 1 [6].

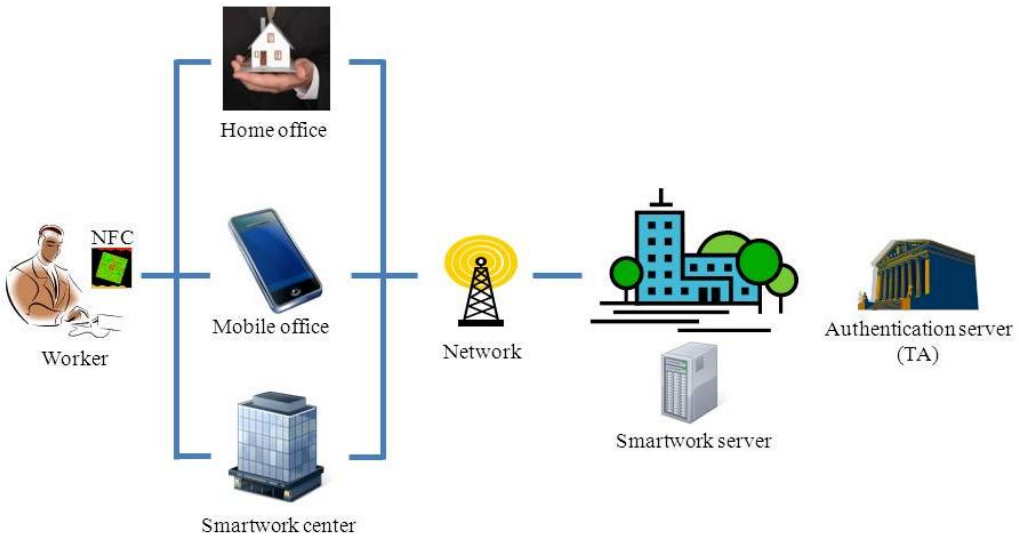

Figure 1. Smartwork Configuration

For the network configuration of the authentication mechanism, we will assume that a worker has NFC and a smart device and a company has a smartwork server with a authentication server as shown in Figure 1.

2.2. NFC Operation Mode

NFC is a short range, < 5cm, wireless communication technology [10-11]. There are three different operating modes, read/write mode, p2p mode and card emulation mode, according to specification as shown in Figure 2.

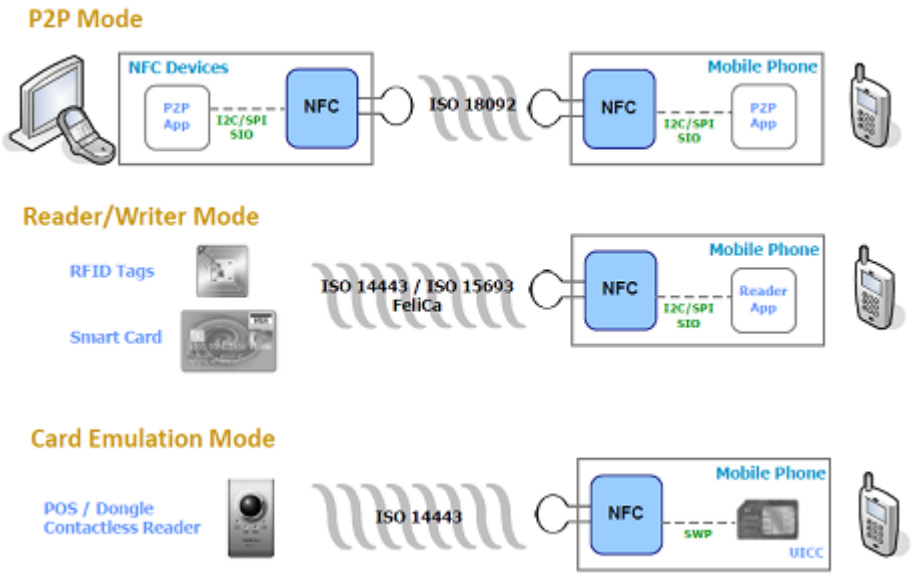

Figure 2. NFC Operation Mode [11]

Read/write mode gives ability to read and write a passive radio frequency identifier (RFID) tag using NFC enabled devices. Common example of utility of this mode is smart poster, which you can get more information/contents from those posters by swiping your mobile device over it. P2p mode is for the communication between two NFC devices. By using this mode, people can exchange data between each other like virtual business cards or photos. The last mode is card emulation mode. These devices can emulate an existing contactless card, which gives a possibility to communicate with contactless reader for example to make a payment by swiping over a payment terminal. This paper only considers the card emulation mode from now on, which is the same concept with the smart card.

3. Won's Authentication Method

This section reviews Won's user authentication method using NFC in smartwork environment and point out security flaws in it [7].

3.1. Review of Won's Authentication Method

This sub-section reviews Won's secure user authentication method using NFC in smartwork environment [7]. Won's method has three phases including user registration, device registration and user authentication. The main key distribution is depending on the trusted authority (TA) as shown in Figure 1. Table 1 defines notations used in this paper.

User Registration: When a worker wants to be registered to the server, he/she submits a smartwork application with *ID* and *PW* to the server by off-line, where *ID* and *PW*

Table 1. Notations

Symbol	Description
ID	Identity of a worker
PW	Password of a worker
DPW	Amplified password of a worker
s	Master key of a server
EK	Authentication key of a worker
SRK	Symmetric key to encrypt *EK*
SEK	Encrypted *EK*
APK	Application authentication key
IMEI	Device identification information
DIMEI	Amplified device identification information
AMK	Device authentication key
R	Random number
M	Message
MAC	Message authentication code
MSK	Session key generated by a mobile device
SSK	Session key generated by a server
USS	Symmetric key between a user and a server
H()	Hash function using SHA-256
E(*K*(*M*))	Symmetric encryption of the message *M* by using a key *K* with AES 256 bits algorithm
$\|\|$	Concatenation operation
$\oplus$	Exclusive OR operation

represent identity and password of the worker. When the application server receives the request, it checks the worker's information and asks for issuing *EK* and *APK* to the authentication server. The authentication server computes $SEK=E(SRK(EK))$, generates *APK* and transmits *SEK* and *APK* to the application server. The application server stores *SEK* and *APK* to the smart card on the employee identification card, which has the NFC functionality.

Mobile Device Registration: A worker installs the smartwork application on the mobile device after downloading. The worker asks a mobile device registration by inputting *ID* and $H(PW)$ to the application server and forwards them to the authentication server. When the authentication server receives the request, it retrieves *APK* by using the worker information and derives $USS=H(APK)$. Separate with the authentication server, the worker inputs *APK* issued previously to the mobile device and computes $USS=H(APK)$. After that, the mobile device sends $M_1=E(USS(IMEI))$ to the authentication server. The authentication server stores *IMEI* after decrypting M_1 and sends success message to the mobile device.

User Authentication: A worker uses the smartwork application on his(her) mobile device to ask a service access by inputting and sending *ID* and $H(PW)$ to the application server. When the application server receives the service access request, it asks user authentication information to the mobile device. The mobile device asks *SEK* on the employee identification card by using NFC function. The NFC transmits *SEK* to the mobile device. The mobile device generates R_1, computer $M_1=E(USS(R_1||SEK||IMEI))$, and transmits M_1 to the authentication server. After receiving the message, the authentication server decrypts M_1 using *USS* and *SEK* using *SRK*, respectively. If the validation of *IMEI* is successful, the authentication server continues the steps otherwise it finishes the communication. The authentication server generates R_2, computes $M_2=E(USS(R_2))$ and sends M_2 to the mobile device. After receiving M_2, the mobile device derives $MSK=H(R_1||R_2)$ after decryption M_2 with *USS*, and sends *MSK* to the server. The server accepts the service access only if *SSK* matches with *MSK*.

3.2 Security Flaws in Won's Authentication Method

In this subsection, we show that Won's authentication method has some security flaws including weak against stolen verifier attack, lack of message integrity and weak against replay attack.

Weak against Stolen Verifier Attack: Stolen verifier attack is possible by an active adversary if he/she could steal the verification table from the server and could read information on it. After acquire the information, the attacker could impersonate as a legal user to the server. Won's method requires to keep a verification table in the server, which needs to keep a set of information { ID, $H(PW)$, APK, $IMEI$ } per user. Thereby, an active attacker could masquerade as a legal user after capture a session message at the user authentication phase and steal the verification table from the server. The attacker could get SEK from the captured previous session message M_1 by using the computed $USS'=H(APK)$ with APK from the stolen verification table. So, the attacker could form $M_1=E(USS'(R_1||SEK||IMEI))$ after generating a random number R_1 and using $IMEI$ from the stolen verification table. There is no way for the authentication server to check this masquerading attack.

Lack of Message Integrity: Message integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data [12]. In Won's method, the mobile device transmits M_1 to the authentication server at the user authentication phase, which is an encrypted message computed by $M_1=E(USS(R_1||SEK||IMEI))$. An active attacker could not know about the contents but could interrupt between two parties by changing some bits on M_1. However, there is no way that the authentication server checks the play from the attacker. In that case, the legal mobile device could not access the smartwork service. It's a very serious design flaw for the company's important work processes.

Weak against Replay Attack: Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack [13]. In Won's method, the authentication server replies M_2 to the mobile device's authentication request at the user authentication phase, which is an encrypted message computed by $M_2=E(USS(R_2))$. Even a passive attacker could capture a session message and replay the session's M_2 to disguise as the authentication server. However, there is no way that the counterpart checks the replay from the attacker. In that case, the legal mobile device could believe that the counterpart is the legal authentication server and established a common session key.

4. Proposed NFC based User Authentication Method

In this section, we propose a NFC based user authentication method in smartwork environment to solve security problems in Won's method. For the secure method design, we set the goals of our user authentication method from [14] as follows

[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 protocol is not based on the tamper resistance assumption of the smart card.

[C5] The protocol can resist various kinds of sophisticated attacks, such as offline password guessing attack, replay attack, denial of service attack, stolen verifier attack and 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 protocol 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 protocol can achieve mutual authentication.

To satisfy those criteria, the proposed authentication mechanism includes user registration, mobile device registration, user authentication and password updating. For the simplicity of the mechanism, the proposed mechanism assumes that the smartwork server could work as the authentication server.

4.1. User Registration

Let *s* denote the server's master key, which is kept secret by the server. When a worker wants to be registered to the server, he/she generates a random number R_U and submits a smartwork application with *ID* and *DPW* to the server by off-line, where *ID* and *DPW* represent the identity and the amplified password computed by $DPW=H(PW||R_U)$ by using the password *PW* of the worker. If the server accepts this request, it will perform the following steps

Step 1 : Computes $Y=H(ID||s)$ and $APK=H(PW||R_U)\oplus Y$.
Step 2 : Stores { *APK*, *H*(), *E*() }to the memory of the smart card on the employee identification card with the NFC function.

After this, the user stores R_U on his/her smart card.

4.2. Mobile Device Registration

A worker installs the smartwork application on his/her mobile device after downloading it. The worker asks a mobile device registration by inserting his/her NFC to the NFC reader and by asking *IMEI* from the mobile device. Overall processes for the mobile device registration are as follows

Step 1 : The worker inputs *ID*, *PW* and *IMEI* to the NFC.
Step 2 : The NFC generates R_{DR} and computes $DIMEI=H(IMEI||R_{DR})$. After that it derives *APK* after computing *DPW* by using the inputted *PW* and the stored R_{UR}, computes $USS=H(Y)$, $M_{DR}=E(USS(DIMEI))$ and $MAC_{DR}=H(USS||M_{DR})$ and sends a mobile device request message { *ID*, M_{DR}, MAC_{DR} } to the smartwork server.
Step 3 : The smartwork server checks the integrity of the message by checking MAC_{DR}. The integrity check is performed by using the derived value $USS'=H(H(ID||s))$. Only if the verification is successful, it computes $AMK=H(DIMEI||s)$ and sends a response message { M_{RM}, MAC_{RM} } to the worker after computing $M_{RM}=E(USS'(AMK))$ and $MAC_{RM}=H(USS'||M_{RM})$.
Step 4 : The NFC sends *AMK* and R_{DR} to the mobile device only if the integrity check of MAC_{RM} is successful.

4.3. User Authentication

A worker uses the smartwork application on his(her) mobile device to ask a service access by inputting and sending *ID* and *PW* to the NFC. The mobile device sends *DIMEI* and *AMK* to the NFC. Overall processes for the user authentication are as follows

Step 1 : The NFC derives *Y* from *APK* after computing *DPW* by using the inputted *PW* and the stored R_{UR}. After that it generates R_{UA} and computes $USS=H(Y)$, $M_{UA}=E(USS(R_{UA}||DIMEI||AMK))$ and $MAC_{UA}=H(USS||M_{UA})$ and sends a mobile device request message { ID, M_{UA}, MAC_{UA} } to the smartwork server.

Step 2 : The smartwork server checks the integrity of the message by checking MAC_{UA}. The integrity check is performed by using the derived value $USS'=H(H(ID||s))$. Furthermore, it checks the validity of the device with $AMK'=H(H(DIMEI||s))$. Only if the verifications are successful, it generates R_{UR} and computes $M_{UR}=E(USS(R_{UA}||R_{UR}))$, $SEK=H(R_{UA}||R_{UR})$ and $MAC_{UR}=H(SEK||M_{UR})$ sends the authentication response message { M_{UR}, MAC_{UR} } to the worker.

Step 3 : The NFC checks the integrity of the message by checking MAC_{UR}. The integrity check is performed by retrieving R_{UR}' by decrypting M_{UR}, establishing a session key $SEK'=H(R_{UA}||R_{UR}')$ and checking whether MAC_{UR} is the same with $H(SEK'||M_{UR})$. Only if the verification is successful, it computes $MAC_{CH}=H(SEK||R_{UR})$ and sends it to the server.

The authentication server checks the validity of MAC_{CH} for the session key establishment.

4.4. Password Updating

Whenever a worker wants to change his/her password, he/she could perform this 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 is as follows

Step 1 : The worker inserts his/her NFC into the NFC reader and inputs *ID*, old password *PW* and a new password *NPW* to the FNC.

Step 2 : The NFC generates a random number R_{NU}, computes $DPW=H(PW||R_U)$ and $NDPW=H(NPW||R_{NU})$ and updates $APK=APK \oplus DPW \oplus NDPW$ and $R_U=R_{NU}$.

5. Security Analysis

This section discusses analysis of the proposed user authentication mechanism for smartwork environment. Although it is important to provide a formal security proof on any cryptographic mechanisms, the formal security proof of authentication mechanisms remains one of the most challenging issues for cryptography research. Until now, a simple, efficient and convincing formal methodology for correctness analysis on security mechanisms is still an important subject of research and an open problem. Because of these reasons, most authentication mechanisms have been demonstrated with a simple proof. Therefore, we follow the approaches used in [15-17]. Table 2 shows security criteria comparison between the proposed mechanism with Won's user authentication mechanism in [7].

Table 2. Criteria Comparison with Won's Authentication Mechanism

Criteria / Mechanism	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
Won in [7]	No	Yes	No	No	No	No	Yes	Yes	No	Yes
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5.1. Offline Password Guessing Attack

Offline password guessing attack is performed after intercepting password related information from the message transmissions in the mechanism and tries to guess the password by offline. However, the proposed mechanism does not use any password related information transmission.

The password related information is 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 mechanism due to the one way hash operation $H()$ used in the password amplification DPW.

5.2. Replay Attack

Replay attack was possible to Won's mechanism due to the lack of session freshness. However, the proposed mechanism uses session dependent random numbers R_{UA} and R_{UR} to cope with this attack. An attacker could intercept the messages { ID, M_{UA}, MAC_{UA} }, { M_{UR}, MAC_{UR} } and MAC_{CH} from the user authentication phase. However, there is no way to the attacker to replay the messages due to the validation check in each step of the phase. So, the proposed mechanism is secure against replay attack.

5.3. Denial of Service Attack

Denial of service attack is an attempt to make a machine or network resource unavailable to its intended users [18]. The proposed mechanism 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 power to modify M in messages. However, there is no way the attacker could get secret key related information in our mechanism. Thereby, our mechanism is safe from denial of service attack.

5.4 Stolen Verifier Attack

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

5.5. User Impersonation Attack

The attacker cannot derive a legal worker's secret information from eavesdropped messages among the worker, 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, using the random number prevents replay of the first message, which could cope from masquerading attack.

Because of using R_{UA} in M_{UA}, the attacker cannot replay the server's message, thus server cannot be masqueraded by malicious attacker.

5.6. Mutual Authentication

Based on the user authentication phase described in Section 4.3, the proposed mechanism can provide mutual authentication among the worker and the smartwork server. In Step 2, by checking the validity of MAC_{UA}, the smartwork server can verify the legitimacy of the worker due to the usage of *USS*. In Step 3, by checking the validity of MAC_{UR}, the worker can verify the legitimacy of the server because only the server could get R_{UA} from the encrypted message to compute *SEK*.

5.7. 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 proposed mechanism uses the hash function $H()$ and the exclusive or operation $\oplus$ to compute a session key depending on the fresh session random numbers. By securing the exchange of R_{UA} and R_{UR}, the worker and the server can separately compute the common session key *SEK*.

6. Conclusion

With the development of IT technology, the interest in smartwork is increasing by using various mobile terminals through Internet services at anytime and anywhere. The introduction of smartwork to a company provides business efficiency, improves productivity and reduces costs, but security researches are required to solve a variety of security issues in it.

The paper reviewed Won's user authentication mechanism and shown the security flaws in it, which are weak against stolen verifier attack and replay attack and have lack of message integrity. Furthermore, we proposed a new NFC based user authentication mechanism to solve the problems and proved the security of the proposed mechanism by using security criteria. As shown in Table 2, the proposed mechanism satisfies all the required criteria in the security mechanism. The proposed mechanism could be used as a basic building block for security on the various smartwork environments.

Acknowledgements

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] K. Scarfone, P. Hoffman and M. Souppaya, "Guide to Enterprise Telework and Remote Access Security", NIST Special Publication, vol. 80, no. 46, **(2009)**.
[2] GSA, Analysis of Home-based Telework Technology Barriers, www.gsa.gov/teleworklibrary, **(2002)**.
[3] K. J. Cha and J. S. Cha, "The Common Challenges to the Successful Implementation of Smartwork Program", International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 2, **(2014)**, pp. 127-132.
[4] Y. Cho, J. Ra, D. Shin and Y. Jung, "The Characteristics of Smartwork Security Compare to Traditional Telework", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 463-468.
[5] Y. Byun and J. Kwak, "Security Management Architecture for Secure Smartwork Center", International Journal of Security and Its Applications, vol. 7, no. 5, **(2013)**, pp. 315-320.
[6] H. Kim, "Investigation on NFC-based Security System for Smart Work", Journal of Security Engineering, vol. 11, no. 3, **(2014)**, pp. 263-272.
[7] D. Won, "A Design of Secure User Authentication Method Using NFC in Smartwork Environment", M. S. Thesis, Soongsil University, **(2012)**.
[8] Naver Knowledge Encyclopedia, http://terms.naver.com/.

[9] MOSPA Smart Work Center, www. smartwork.go.kr.
[10] NFC, NFC Forum Technical Specifications, http://members.nfc-forum.org/specs/spec_list/.
[11] http://blog.myti.it/post/6036601997/nfc-operating-modes.
[12] http://en.wikipedia.org/wiki/Data_integrity.
[13] http://en.wikipedia.org/wiki/Replay_attack.
[14] S. Park and H. J. Park, "Privacy Preserving Three-party Authenticated Key Agreement Protocol using Smart Cards", International Journal of Security and Its Applications, Accepted for the publication, **(2014)**.
[15] H. Kim, "Location-based Authentication Protocol for First Cognitive Radio Networking Standard", Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 1160-1167.
[16] H. Kim, "Freshness Consideration of Hierarchical Key Agreement Protocol in WSNs", International Journal of Security and Its Applications, vol. 8, no. 1, **(2014)**, pp. 81-91.
[17] H. Kim, "End-to-End Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks", International Journal of Security and Its Applications, Accepted for the publication, **(2014)**.
[18] http://en.wikipedia.org/wiki/Denial_of_service_attack.

Authors

Hyunsung Kim, he is a full 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.

Sung Woon Lee, he 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.

