International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.237-248
http://dx.doi.org/10.14257/ijsia.2016.10.10.22

Enhanced User Authentication Method Using USB Device Information

Jin-Hae Lee[1], Seon-Joo Kim[*2], Jin-Woo Lee[3], Jin-Mook Kim[4] and In-June Jo[5]

[1,3,5]*Dept. of Cyber Security, PaiChai University*
Doma 2-dong, Seo-gu, Dajeon-City, 302735, KOREA.
[2]*Information Security Evaluation Dept. TTA,*
47 Bundang-ro, Bundang-Gu, Seongnam-City, Gyunggi-do, 13591, KOREA
[4]*Division of IT Education, Sunmoon University,*
221 bun-gil 70, Tangjeong-myon, Asan-si, Chungchungnam-do, 31460, KOREA
[1]*ljh1852@pcu.ac.kr,* [2]*sunjoo@tta.or.kr,* [3]*shon89@pcu.ac.kr,*
[4]*calf0425@sunmmoon.ac.kr,* [5]*injune@pcu.ac.kr*

Abstract

We are accustomed to using various multimedia services through authorization as a legitimate user, by entering ID and password. However, while technology using ID and password in that case, is inexpensive for constructing system, and convenient for general public to use, user ID and password can be easily exposed to attackers by various attacking techniques, such as password guessing attack, reply attack, and others[1]. In order to resolve such problems, users can be authenticated by adding other authentication methods, such as security card, OTP, certification, finger print recognition, and others, to user authentication using ID and Password [2-5]. In this thesis, we suggest user authentication method that uses authentication data stored in USB memory after generating authentication data by combining USB memory info and user password in multimedia environment. In such system, even if attacker takes over user authentication data stored in USB memory, USB memory device info is still unknown, and thus, seized information cannot be used. In addition, it is convenient to use due to inexpensive construction cost and regular USB memory. Therefore, in the future, it is expected to provide easy construction and operation environment to the companies required to use ID and password based authentication.

Keywords*: User Authentication, ID/PW based, USB Device information, USB Container ID*

1. Introduction

Digital certificate used frequently in Korea has been promoted since establishment of e-Commerce Law, but it became inconvenient in many ways, such as recently added requirements of Active-X installation, and limited support to special browsers. However, while certificate based user authentication technique provides high stability, its convenience in terms of construction, operation, and usage are not favorable. User authentication method in multimedia environment include various technologies such as ID and password, authentication certificate, finger print recognition, Enhanced Password Based User Authentication Mechanism[6], and others[7]. Even so, ID and password based authentication is the system that enables inexpensive build up, and convenient use in multimedia environment. In this research, we suggest a method to authenticate user using fixed type of password and USB memory device info, in addition to user friendly ID and password method.

* Corresponding Author

ISSN: 1738-9976 IJSIA

2. Related Researches

2.1. Technology of User Authentication

In user authentication technology, a user can be authenticated using the methods known to or owned by only users, such as user password, security card, OTP, finger print, and others. Most frequently used technology is the method using ID and password. However, ID and password is vulnerable to various hacking attacks [8]. Besides this method, there are many kinds of methods including security card, OTP, mobile phone and email certification, finger print recognition, and others. As security card uses only limited number of security figures printed, there was a case exposed to a hacking attack targeting at such vulnerability. Furthermore, OTP or certificate can be safe by using one time use password or secure public key based structure, but it is not economical due to expensive system build up and operation costs. While the method using human body such as finger print or iris is considered the safest way, system build up and operation is expensive, and authentication data cannot be changed even when personal info is exposed by hacking attacks.

2.2. USB Memory Device Overview

USB (Universal Serial Bus, hereinafter referred to as "USB") refers to standard specification to connect computer peripherals [9, 10]. USB memory combines semi-conductor Flash Memory that can save and store data, and USB, which means data transfer specification. USB memory is easy to carry due to features of compact size and light weight, and files can be easily moved/copied/deleted by connecting with USB port only. As shown in [Figure 1], internal structure of USB memory is comprised of ①Flash memory ②Controller ③USB connector. ①When using flash memory, data can be stored and deleted easily, and protected even when power supply is cut off. ②Controller takes control on data transmission between flash memory and USB connector. ③USB connector plays roles of power supply and data transmission medium in connection with PC, and USB ports of various IT equipments. While this USB memory offers convenience of portability, there is a risk of data exposure stored in USB memory when it is lost, and the data stored in USB memory can be easily moved/copied to external system by malicious codes [11] immediately when USB memory is connected with PC.

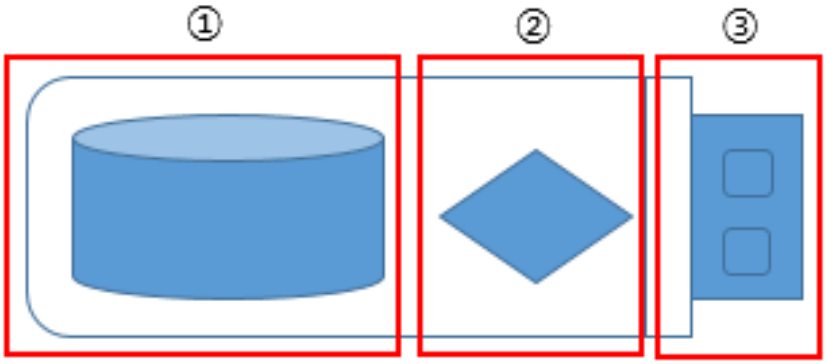

Figure 1. USB Memory Structure

2.3. Load Process of USB Memory Device

A data load process from USB memory device is shown in Figure 2.

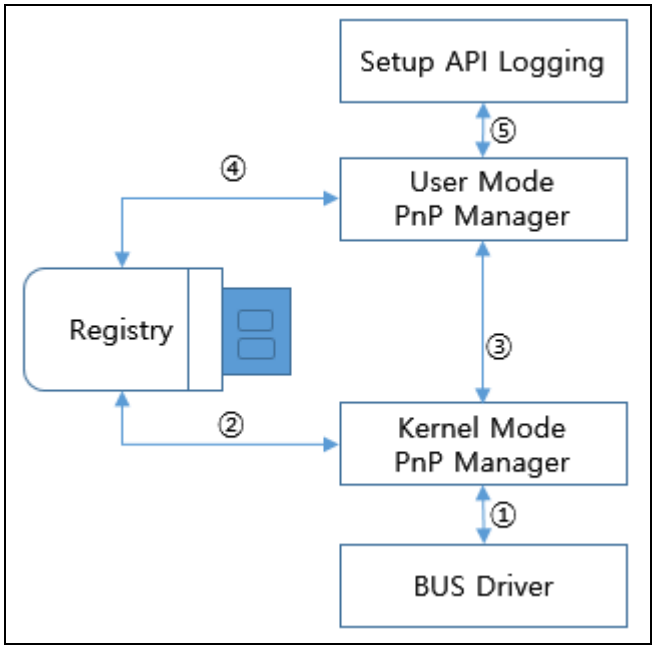

Figure 2. Load Process of USB Memory Device

① When we connect USB memory to PC, the Bus Driver sends of USB memory's device descriptor to Kernel PnP Manager.
② Kernel PnP Manager sets up Device Class ID based on USB memory's device descriptor and then searches USB's driver from registry.
③ Kernel PnP Manager loads USB's driver, if that driver is found in the registry. However, unless driver exists, User mode PnP manager from firmware of USB's device and then records in the registry.
④ User mode PnP Manager installs the USB's driver to PC.
⑤ User mode PnP Manager sets up the driver of USB memory and then connects correspond USB memory device to storing. It records USB memory information in the registry. At this time, refer to [table 1] - related USB memory device descriptor saved in registry. Related USB memory information preserved in registry. that is, device class ID, unique instance ID, Vendor ID, product ID and serial number are utilized in operating system it creates and uses USB container ID[12] formed string which can be made use in the operating system [8]. Refer to Figure 3. USB container ID value created the time when USB memory device puts PC.

Figure 3. Example of USB Container ID

The OS realizes only USB device through USB container ID value and identifies device connected USB port then performs function fitted correspond device as per type of that such as keyboard, mouse, USB memory device.

Table 1. USB Memory Information

Identifier	Explanation
Device class ID	Identifier which is made by using form of USB memory device, name of manufacturer and product and version.
Unique instance ID	If Instance ID that is serial number of USB memory device doesn't include serial number, OS will be made that randomly.
Vendor ID (Product ID)	Manufacturer of USB memory and identifier of product
Volume serial number	Volume serial number for USB memory device
Initial connection time	Time information putting first USB memory device to system
Initial connection time after boot up	Time information connecting first USB memory device after system boots up.
Final connecting time	Time information connecting last USB memory device

3. The Proposed Method

This thesis proposed method that can protect user authentication data safely even when user ID and password are exposed or user authentication data is copied/moved, by improving security vulnerability of ID/PW method, and using USB memory device information [13]. In line with that, user used USB Container ID as user authenticating element, after saving user authentication data by using container ID in USB memory. Followings are notation of the used signs.

Table 2. Procedure Notation

ID	User's Identifier ID
PW	User's Password
CID	User's USB container ID
es_key	Session Key encryption key
s_key	Session Key
PRNG	Pseudorandom Number Generator
$E_n(M)$	n in key symmetric encryption to M

$D_n\{M\}$	n in key symmetric decrypt to M
(A || B || C ……)	String consisted of items(a, b, c)
(A + B + C ……)	Record consisted of items(a, b, c)

3.1. User Registration Procedure

In this section, there is a description of the process in which a user is registered to the application system to be used. The procedures for registering the user are shown in Figure 4.

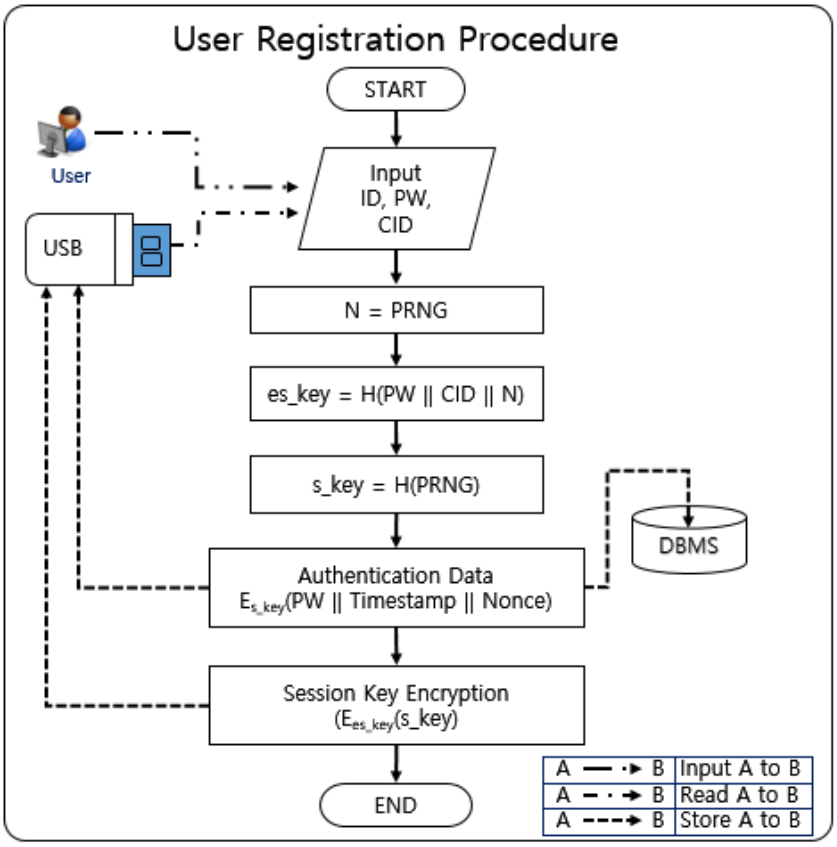

Figure 4. User Registration Procedure

Step 1) The User input ID/PW, and then load USB Container ID(CID) from user's USB Memory device.

Input (ID, PW), Read(CID)

Step 2) It generate a pseudo random number(N) from PRNG function.

N = PRNG

Step 3) Generate a session-encryption key(es_key) which results from the one way hash function using the input values, User's PW(PW), USB Container ID(CID) and the random number(N) generated in Step 2. This key is used to encrypt the session key(s_key) used to encrypt the authentication data valid for only one session.

es_key = H(PW || CID || N)

Step 4) Generate Session key(s_key) from PRNG. The s_key is session key.

s_key = PRNG

Step 5) Encrypt the user authentication data by using the session key (s_key). PW is the password of the user, the Timestamp is the session datetime, the Nonce to protect the reproduction of the registered session authentication data.

E_{s_key}(PW || Timestamp || Nonce)

Step 6) Store the encrypted authentication data generated in step 5 to DBMS / USB.

Step 7) For preventing session key from exposing, session key-encryption key generated in Step.3 encrypts session key.

E_{es_key}(s_key)

Step 8) Store the encrypted session key in step 7 to USB.

3.2. User Authentication Procedure

In this section, we explain the specific procedures for authenticating the user registered in the preceding section to allow him/her to access the system. The procedures for authenticating the user are shown in Figure 5.

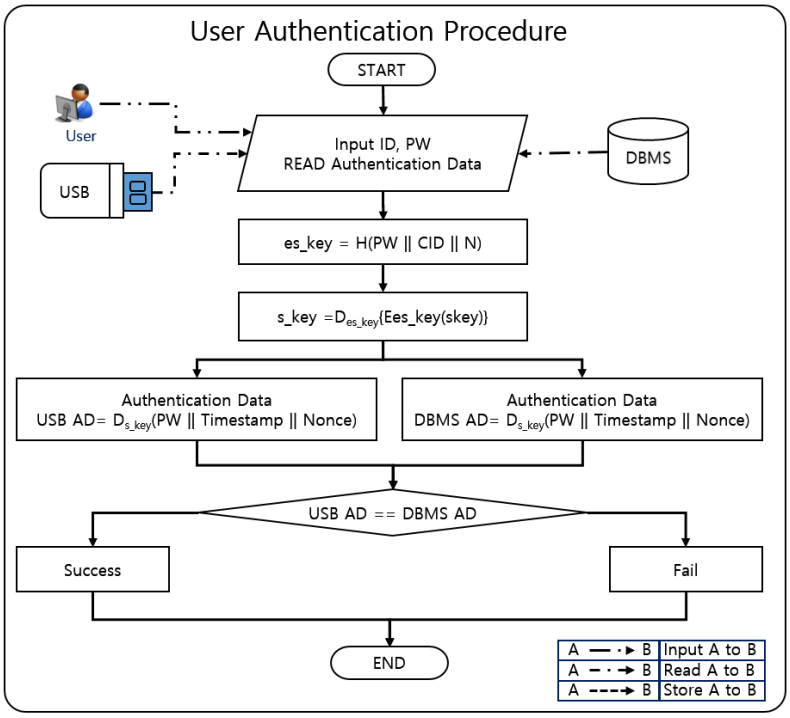

Figure 5. User Authentication Procedure

Step 1) The user input the ID/PW, and load the authenticate data from USB memory.

Input (ID, PW)

Step 2) regenerates the session-encryption key (es_key) which has previously resulted from the one-way hash function using the input values, the random number(N), the password(PW) and USB Container ID(CID).

es_key = H(PW || CID || N)

Step 3) decrypts the encrypted session key Ees_key (s_key) by using the session-encryption key (es_key) recreated in Step 2.

$s\_key = D_{es\_key}\{E_{es\_key}(s\_key)\}$

Step 4) For creating USB memory Authentication Data(USB AD), decrypt authentication data(Ds_key(PW|| TimeStamp || Nonce)) which is encrypted s_key on Step 3.

$USB\ AD = D_{s\_key}\{E_{s\_key}(PW \| TimeStamp \| Nonce)\}$

Step 5) Load authentication data which is saved database in application system. DBMS.

$READ(E_{s\_key}(PW \| TimeStamp \| Nonce))$

Step 6) For making Database Authentication Data(DB AD), encrypted authentication data which is read on Step 5 decrypt session key(s_key).

$DB\ AD = D_{s\_key}\{E_{s\_key}(PW \| TimeStamp \| Nonce)\}$

Step 7) If the authentication data decrypted in Step 4 is the same as the authentication data decrypted in Step 6, the authentication is successful; otherwise, the authentication is failed.

3.3. User Authentication Data Reconfiguring Procedure

In this section, there is a description of the process in which the user successfully authenticated in Section 3.2 reconfigures the authentication data for the next authentication session. The procedures for reconfiguring the authentication data are shown in Figure 6.

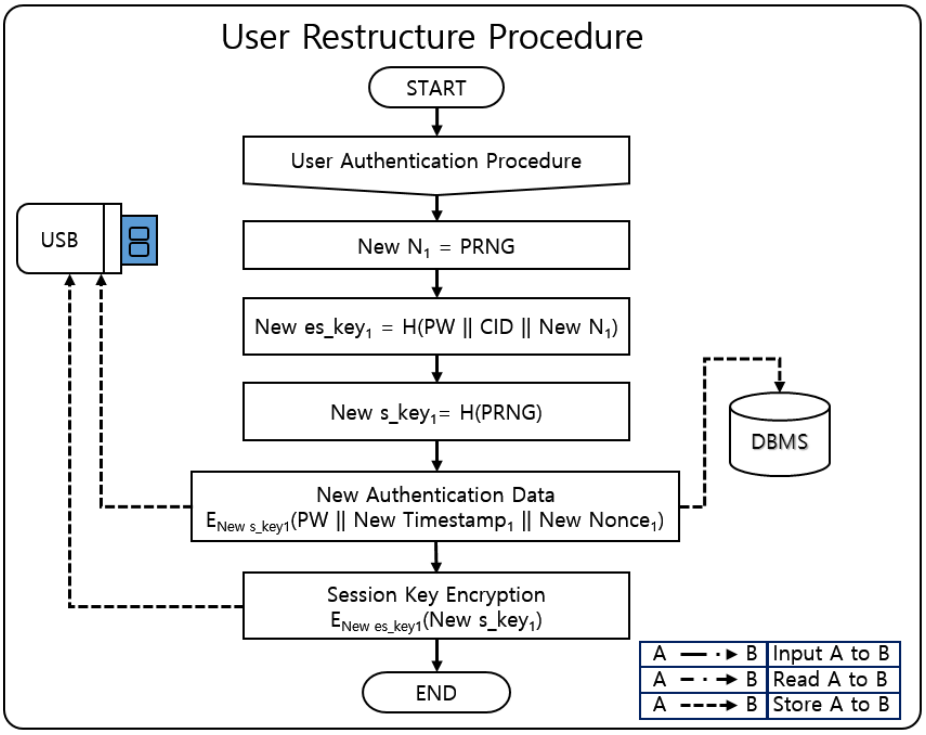

Figure 6. User Restructure Procedure

Step 1) If authentication matches up on Section 3.2 User Authentication Procedure, it will go through restructuring steps of authentication data. Start to restructure with user's ID(ID), user's password(PW) and USB Container ID(CID) loaded before stage.

Step 2) It generate a new pseudo random number(New N_1) from PRNG function.

New N_1 = PRNG

Step 3) Generate a new session-encryption key(New es_key_1) which results from the one way hash function using the input values, User's PW(PW), USB Container ID(CID) and the random number(New N_1) generated in Step 2. This key is used to encrypt the session key(s_key) used to encrypt the authentication data valid for only one session.

New es_key_1 = H(PW || CID || New N_1)

Step 4) Generate New Session key(New s_key_1) from PRNG. The New s_key_1 is session key.

New s_key_1 = PRNG

Step 5) Encrypts the user authentication data by using the session key (New s_key_1). PW is the password of the user, the New Timestamp is the session datetime, the New Nonce to protect the reproduction of the registered session authentication data.

$E_{New\ s\_key1}$(PW || New Timestamp || New Nonce)

Step 6) Update the encrypted authentication data generated in step 5 to DBMS / USB.

Step 7) For preventing session key from exposing, session key-encryption key generated in Step.3 encrypts the New session key.

$E_{New\ es\_key1}(New\ s\_key_1)$

Step 8) Store the encrypted session key in step 7 to USB.

4. Evaluation

In this thesis design to secure safety in system requiring user authentication, and to use at inexpensive price. Therefore, outstanding safety and convenient usability of proposed system need to be described objectively in comparison with existing user authentication method.

In this chapter, we compare the ID/PW based user authentication method used in system, certificate [3], finger print recognition, OTP [14], and others.

Table 3. Comparing Existing-System with Proposed System

	ID/PW	Certificate	Fingerprint	OTP	Proposed System
Characteristics	Static	Static	Static	Dynamic	Dynamic
Password Change	Necessary	Necessary	-	Unnecessary	Unnecessary
Reusability	Possible	Possible	Possible	Impossible	Impossible
Cost	Low	High	High	High	Low
Protect authentication data	No	No	No	Yes	Yes
Protect Password	No	Yes	-	Yes	Yes

As show in Table 3, The proposed system has a number of features. First, user authentication data of proposed method and OTP based method has a dynamic characteristics, but the others has static characteristics. Second, require continuous password change in user authentication method, ID/PW and Certificate, but proposed system and OTP do not need to change password. Third, the OTP and proposed sysem changes each time, used authentication data cannot be reused, but the others can be reused. Fourth, the system building cost is inexpensive because ID/PW method and proposed system can be build only if there is a storage system to save authentication data. However, other authentication systems are expensive as those requires additional system or hardware equipments. Fifth, If the certificate method is exposed cannot be used, there is no way to protect the exposed authentication data. However, since the proposed method is protected using USB device info, the authentication data cannot be used even after the exposure. Sixth, other authentication data can be used the exposure of password in user authentication method, for certificate, authentication data cannot be used once

password is exposed. However, with proposed method, authentication data can be used only by combining USB device info and user password even after password exposure. Thus, the authentication data cannot be used despite the password exposure. Accordingly, since proposed method generates user authentication method by combining USB device info and user password, it has the security level equivalent to certificate, finger print recognition, and OTP. In addition, proposed method has the advantages of inexpensive construction price and convenience just as ID and password method.

5. Conclusions

User authentication comes with various technologies, such as ID and password, OTP, certificate, finger print, and others. However, safety management plan of user authentication data is necessary, as there are on going security accident occurrences taking over user authentication data, through sniffing, malicious code, pharming site, and others. In such plan, various technologies is suggested and utilized, such as USIM smart authentication technology using Smartphone [13], certificate based user authentication [3], Management Method to Secure Private Key using OTP [14], and others [15].

In this thesis, suggested method was designed considering vulnerability, cost, and convenience of existing authentication methods. Considering convenience of ID and password method, user authentication is carried through user ID and password, USB Container ID. User authentication data changes automatically without changing user's password, as authentication data changes automatically whenever logging in. Thus, user does not have to change password periodically. Besides, using additional authentication element of USB Container ID, user authentication data can be protected safely, even if user authentication data file is copied/moved, or user password is exposed. Lastly, because we don't have to build additional system, different from security card, OTP, certificate, finger print, and others, it has advantages of low construction cost.

This method can be applied ID and Password method immediately, and is expected to make great deal of progress in terms of security in existing multimedia environment. For details of further study, as authentication data cannot be restored, and user authentication is impossible, if user USB memory device is lost, supplementary research is necessary in that regard.

References

[1] J. Kwak, W. Hong and W. Yi, "Vulnerability and Security Requirement Analysis on Security Token and Protection Profile Development based on Common Criteria Version 3.1", Journal of the Korea Institute of Information Security and Cryptology, vol. 18, no. 2, **(2008)**, pp. 139-150.
[2] K.-c. Kim, "The reason for evading security card: Electronic financial supervision regulation is contributed to attack", Slow News, http://slownews.kr/12222.
[3] I. Kim, J. Hwang and W. Park, "A Study on Enforce the Policy of User Certification in Public Certificate System", Journal of Korea Convergence Security Association, vol. 10, no. 4, **(2010)**, pp. 69-76.
[4] J. Lee, H. Kwon and J. Lim, "A Study on Certificate-based Personal Authentication System for Preventing Private Information Leakage through Internet", Journal of Korea Convergence Security Association, vol. 10, no. 4, **(2010)**, pp. 1-11.
[5] H. Lee and J. Kim, "Quality Evaluation Model about Efficiency for Fingerprint Recognition System", Journal of Digital Convergence, vol. 12, no. 6, **(2014)**, pp. 215-221.
[6] S. Kim, J. Na and S. Son, "Password Authentication Protocol Trends", Electronics and Telecommunications Trends, vol. 16, no. 6, **(2001)**, pp. 41-48.
[7] S.-y. Kim, S.-j. Kim and I.-j. Jo, "Enhanced Password Based User Authentication Mechanism Using Mobile Storage", Journal of the Korea Contents Association, vol. 14, no. 11, **(2014)**, pp. 533-540.
[8] Y.-h. kim, S. Lee and H.-j. Jang, "A Study on Taxonomies of User-Authentication Methods", Journal of Security Engineering, vol. 4, no. 1, **(2007)**, pp. 17-24.
[9] S.-w. Lee, "The standard for connecting with peripherals, USB", IT DongA, http://it.doga.com/21688.
[10] USB Flash Drive, https://ko.wikipedia.org/wiki/USB.

[11] H. Seo, J. Choi and P. Chu, "Design of Classification Methodology of Malicious Code in Windows Environment", Journal of the Korea Institute of Information Security and Cryptology, vol. 19, no. 2, **(2009)**, pp. 83-92.
[12] Container ID Overview, MSDN, https://msdn.microsoft.com/en-s/library/windows/hardware/ff540024(v=vs.85).aspx.
[13] J. Lee, "An issues certificates used in smart environments", Internet & Security Focus, **(2013)** March, pp. 23-53.
[14] S.-j. Kim, I.-j. Jo, "Management Method to Secure Private Key of PKI Using One Time Password", Journal of the Korea Contents Association, vol. 14, no. 12, **(2014)**, pp. 565-573.
[15] J.-H. Lee, S.-J. Kim, J.-W. Lee, J.-M. Kim and I.-J. Jo, "The User Authentication method based on the USB device information2016 10th International Workshop on Psychology and Counseling Welfare Security, Reliability and Safety, vol. 6 **(2016)**, pp. 32-35

Authors

Jin-Hae Lee, he received B.S in computer engineering from Paichai University, Daejeon, Korea, in 2015. Currently, He is in the Master's course in Cyber Security in same university. His research interests include network security, security engineering, cryptology, Software Development.

Seon-Joo Kim, he received the Ph.D. in computer engineering, network security from Panchal University, Daejeon, Korea, in 2013. Currently, He is a research engineer in the Information Security Evaluation Dept. at the Telecommunications Technology Association (TTA). His research interests include security testing and Common Criteria.

JinWoo Lee, he received B.S in computer engineering from Paichai University, Daejeon, Korea, in 2015. Currently, He is in the Master's course in Cyber Security in same university. His research interests include network security, security engineering.

Jin-Mook Kim, he received the Ph.D. in computer engineering, computer security and authentication from the Kwangwoon University in 2006. Currently, He is an assistant professor in the Division of IT Education at Sunmoon University in Korea. His research interests include network control architecture, security engineering, authentication on the network, and Smart-phone security.

In-June Joe, he received the Ph.D. in computer engineering from Aju University, Suwon, Korea, in 1999. He has been working research engineer in the ETRI from 1983 to 1994. Currently, He is a professor in the Dept. of Cyber Security at Paichai University in Korea. His research interest include network security, security engineering, user identification and authentication.