International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:10, 2014

A Study on User Authentication Method Using Haptic Actuator and Security Evaluation

YoHan Choi, HeeSuk Seo, SeungHwan Ju, SungHyu Han

***Abstract*—**As currently various portable devices were launched, smart business conducted using them became common. Since smart business can use company-internal resources in an exlternal remote place, user authentication that can identify authentic users is an important factor. Commonly used user authentication is a method of using user ID and Password. In the user authentication using ID and Password, the user should see and enter authentication information him or her. In this user authentication system depending on the user's vision, there is the threat of password leaks through snooping in the process which the user enters his or her authentication information.

This study designed and produced a user authentication module using an actuator to respond to the snooping threat.

***Keywords*—**Actuator, User Authentication, Security Evaluation.

I. Introduction

RECENTLY, as various mobile devices such as smart phones and tablet PCs have been released, an access to information became easier compared to the past. As information can be accessed in various methods, the protection of the information becomes more important, and especially, importance is attached to the security of the user's private information and enterprise's important information [1]. To approach such information, user authentication is an essential element

User authentication includes one based on the knowledge the user is aware of; one based on possession using the authentication medium the user owns; and bio authentication using the user's physiological characteristics [2]. In user authentication using only one of these authentication methods, information may leak by a malicious user [3], [4]. To solve demerits occurring in the use of single authentication method, a multi-factor authentication method using two or more authentication methods rather than one method has been suggested since each authentication method has pros and cons. The multi-factor authentication can secure stability of user authentication increasing the complexity of the authentication process.

This study carried out an inquiry into a two-factor authentication method using the password the user is aware of and the user authentication module he or she owns. This uses tactile sensation information delivered from the authentication module the user has as authentication information. This study used an authentication module with a size of a finger joint to implement an input and secured stability from a snooping attack.

YoHan Choi, HeeSuk Seo, SeungHwan Ju, and SungHyu Han are with the Korea University of Technology and Education, Cheonan-si, Chungnam 330708 Korea, Republic Of (phone: +82-41-560-1495; fax: +82-41-560-1462; e-mail: {yhchoi, histone, judeng, sunghyu}@koreatech.ac.kr).

In the user authentication module, an actuator was added to deliver information through the user's tactile sensation. The actuator used for the user authentication module was a solenoid type linear actuator in which 12 pins could operate individually. This performs user authentication receiving an input of a password the user knows if a specific number or a tactile sensation pattern is presented to the user through an authentication module.

II. Related Work

A. User Authentication Using Haptic Keypad

Reference [7] proposes a user authentication method through the Secure Haptic Keypad (SHK) resistant against a snooping attack that may occur in a user authentication process. This pro-vides users with vibration patterns using physically separated 3 haptic buttons.

For user authentication, different vibration patterns from 3 keypads respectively are delivered to a user's tactile sensation and the user performs user authentication by pressing a haptic button that sends a vibration pattern he or she set among 3 types of vibration patterns. The vibration pattern generated in each button generates one random pattern out of the predefined 6 types of patterns and user authentication is carried out by the user pressing the keypad for the order of his or her designated vibration patterns.

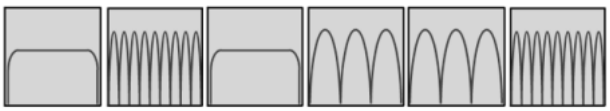

Fig. 1 The iconic tacton PIN notation: a 6 item PIN with the following tactons: Cont., 2Hz, Cont., 1Hz, 1Hz, 2Hz

B. Haptic and Audio PIN Input Technique

User authentication performed in a situation where there are a lot of people around has a lot of threats of exposure of the authentication information. Reference [8] proposed several methods of user authentication using the user's tactile sensation or audio information to solve this problem.

This is a method of using SHAKE SK6 for authentication. SK6 delivers data to the authentication terminal by Bluetooth and with the system by Wi-Fi. SK6 delivers haptic information through vibration to a user and the user enters PIN information with a dial method. The user may set up 4 to 6 digits for PIN information and set up a number out of 1 to 10 either clockwise or counterclockwise as his or her PIN. In addition, it was designed so that the user could cancel his or her inputs by

shaking the device.

Fig. 2 Shake SK6 unit

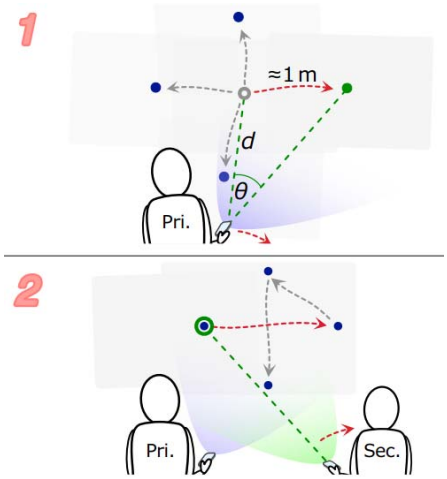

Fig. 3 Estimating participants' positions

C. Generation of OTP Using Fingerprint

Reference [9] proposes a method of generating OTP using a user's fingerprint. This generates OTP using the user's unique fingerprint information, which safer than the existing method of generating OTP using a secret key.

This does not use the fingerprint information as it is, but uses the user's scanned fingerprint information characteristics to generate OTP so that the user's bio information can be used safely. Using the difference between the position and angle generated whenever a user's fingerprint is scanned, different key values can be generated from the same fingerprint, and using this, a different encryption key is generated each time.

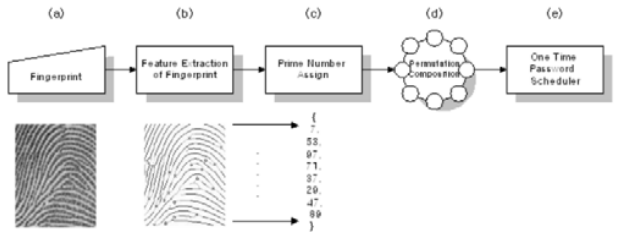

Fig. 3 Creation of Password keys using Fingerprint Characteristics

III. User Authentication Using Tactile Sensation

A. Overview of User Authentication Module

In general, for user authentication, methods of entering a 4-digit or 6-digit PIN are used. The user authentication through a PIN has merits that a user can easily remember and that the implementation is simple. However, it has demerits that the process in which the user enters the PIN with a keypad can be exposed easily by peeping and that a malicious person can find the number used by the user using the fingerprint information that remains in the keypad and combine this to infer the PIN information [5], [6].

This study designed a PIN input method using a user's tactile sensation. This uses a haptic actuator as a device of delivering information to the user and receiving an input from the user.

It got rid of a possibility of peeping the process in which the user enters PIN information next to him or her by delivering the information using the haptic actuator on the user's finger tip.

Entering the PIN information using the haptic actuator has a threat of a possibility of inferring the information entered by a user by measuring the time interval consumed to enter the PIN information. To eliminate those threats, the order of the numbers presented to the user by the haptic actuator was made irregular. By differing the order of the numbers output through the haptic actuator and making the time taken to enter the PIN information by the user irregular, an attacker could not infer the user's password.

B. Haptic Actuator Module

The haptic actuator used in this study is a solenoid type linear actuator. To facilitate the assembly of the solenoid actuator, it was developed in a cylindrical structure. It consists of a stainless housing for the exterior of the actuator, a steel housing for the path of magnetic flux, solenoid coil, that is its driving force, a steel cover designed to fix the solenoid coil and connect the line from the outside and a steel plunger with a vertical motion following the current in the coil in the steel housing.

This study made actuators like Fig. 4. Two 2*3 actuators were combined to form a 4*3 array type actuator. To secure the ease of assembly of the actuator, it was separately assembled, and 12 pins can independently be controlled and operated at a different frequency in the actually assembled actuator. This study controls the actuators made and delivers number information to a user, but each actuator is separately adjustable, so besides numbers, brailles, texts and shapes can be used. This can increase the number of occasions to combine and al-lows the user to generate and use a complex PIN.

The size of the actuator input module used in this study was 15.4mm*9.2mm.

A small actuator input module can be produced in a smart phone case. By making the input module small, it is easy to be applied to mobile devices and be made in a case form for existing mobile devices. Making the actuator small and modular can reduce the economic burden occurring in the process of introducing a password input module using an actuator.

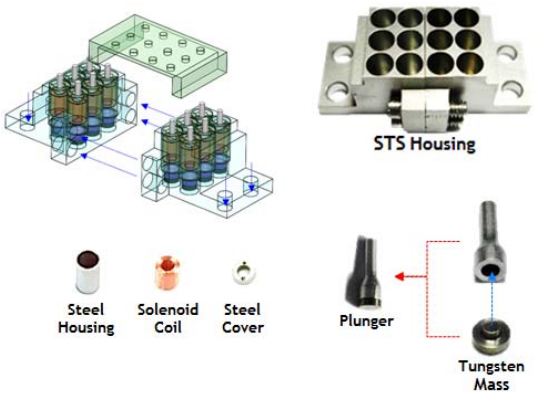

Fig. 4 4*3 array type actuator

C. Haptic Actuator Module

The haptic actuator authentication module is used in combination with a user's mobile terminal. In the process of user authentication, the mobile terminal controls the actuator.

The user authentication using a haptic actuator consists of an actuator controller that can control the actuator and an authentication operator to perform authentication using the information entered by a user and control the actuator.

An output number synthesizer included in the authentication operator performs the combination of the output sequences of the number presented to a user through the actuator controller.

The order of output is changed by the output number synthesizer so that it is used to get rid of the threat of inference of the time taken to enter a password and find out a password. By changing the time taken when a user enters a password by each unit, the threat of guessing the password can be reduced.

An authentication execution unit performs user authentication using the information entered by a user. To judge the user's input, the change in the distance the actuator has moved is measured. The authentication execution unit stores the value entered by the user and delivers it to the authentication system or performs authentication itself.

The actuator motion controller included in the actuator controller controls the actuator's operation. To control 12 pins included in the haptic actuator authentication module independently, it has information about each actuator and the actuator arrangement, and it moves each pin according to the order of the combination in the output number synthesizer and provides the user with haptic information.

A user feedback unit detects the pressure by which a user presses the haptic actuator and check to what number the user responds.

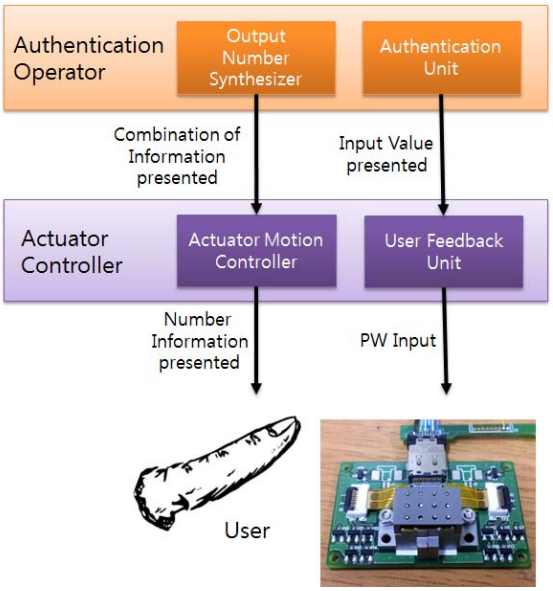

Fig. 6 Authentication Process

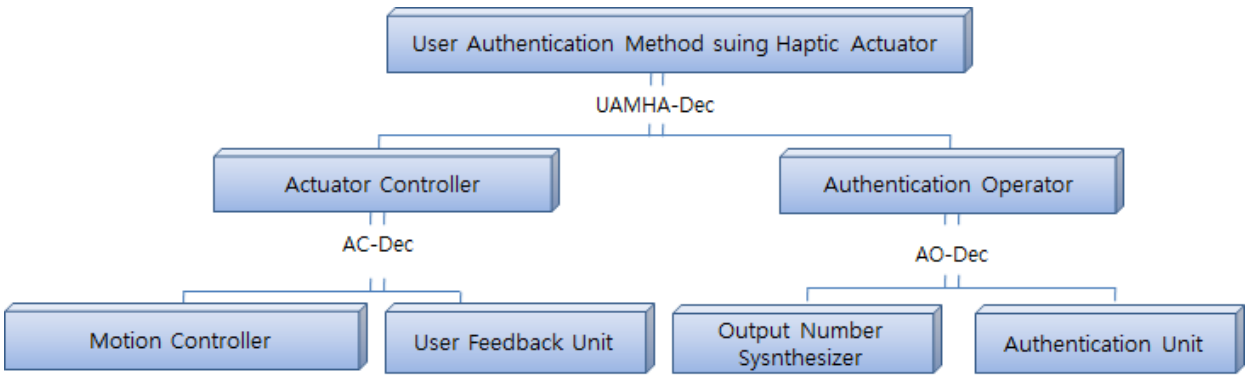

Fig. 5 Structure of User Authentication Module

D. User Authentication Process

The process of performing user authentication using a haptic actuator is as follows:

The user authentication process begins from a user's request for the authority to access the information system.

The authentication system checks if the user's haptic actuator module is a device registered in it. If information about the relevant device has not been registered in the system, the

authentication would fail.

If the haptic actuator is one registered to the authentication system, the system receives the information necessary for the user authentication from the user and verifies the user.

The output number synthesizer defines output sequences in order to combine the output sequences of the number presented by an actuator so as to receive authentication information from the user. The number delivered to the user is provided randomly so as to reinforce security by presenting the time taken when the user enters a certain number irregularly.

To deliver information to the user according to the order combined in the output number synthesizer, the actuator motion controller controls 12 pins and presents numbers to the user.

If the user presses the actuator correctly for the PIN he or she defined in advance, the user feedback unit detects the user's input and delivers the number presented when the user pressed the actuator to the authentication unit.

The authentication operator encodes PIN information obtained from the user to deliver to the authentication system, which verifies the user authority based on this information.

If the user authentication succeeds, the system grants the access authority requested by the user so that he or she may use the system resources or obtain an authority.

E. User Authentication Algorithm and Security Evaluation

The detailed algorithm of user authentication using an actuator is applied by modifying the signature method using a well known ID. The values used in the authentication process are as follows:

n : product of great prime numbers and randomly selected

e : Euler's function value of n , $\varphi(n)$ and a relatively prime random number

H : hash function

ID_i : ID of each user i

PW_i : Password of each user i

A_i : value satisfying $A_i \equiv (PW_i)^e (mod\ n)$

Among the above values, n, e, H, ID_i and A_i are disclosed, PW_i is one known only by user i, and p and q are values known only by the authentication system. The authentication process is as follows: The actuator receives ID_i and PW_i from a user and generates a random number k. And it performs the following calculation.

$$S \equiv K^e (mod\ n)$$
$$T \equiv PW_i \cdot S^{H(s,ID_i)} (mod\ n)$$

And it delivers the above values, S, T and ID_i to the authentication system. The authentication system checks if the following formula has been established to verify user authentication.

$$T^e \equiv A_i \cdot S^{H(s,ID_i)} (mod\ n)$$

The above expression is established as follows.

$$\begin{aligned} T^e &\equiv (PW_i \cdot k^{H(s,ID_i)})^e (mod\ n) \\ &\equiv PW_i \cdot k^{e \cdot H(s,ID_i)} (mod\ n) \\ &\equiv A_i \cdot S^{H(s,ID_i)} (mod\ n) \end{aligned}$$

The stability of the above algorithm is based on the fact that it is difficult to find PW_i that meets

$$A_i \equiv (PW_i)^e (mod\ n)$$

in other words, it is difficult to find the eth square root of PW_i . And yet, if factorization in prime factors of n is known, using the Chinese Remainder Theorem, the eth square root of PW_i can be found. Therefore, the security of this algorithm is based on the fact that it is a very difficult to factorize n, the product of p and q in prime factors when prime numbers p and q are very large numbers.

IV. Conclusion

This study produced a password input module using an actuator and composed a user authentication module. It evaluated performance and tested user authentication process through an algorithm.

Existing studies on password used mainly for user authentication are concentrated on the user's vision. These studies are very useful for the public without any disability, but otherwise, the applications are very difficult and there is a demerit that they are very vulnerable for a snooping attack that can occur in the process of entering a password.

This study secured strong security for the snooping attack that can occur in the password input process using an actuator. In addition, the order of the number presented to a user by the actuator was changed each time so as to make the time when the user enters the number irregular. By changing the time when the user enters the number, the threat of a leak of the password by measuring the time to enter it was eliminated.

A password input module using an actuator was produced with a size available in a mobile device. It can be applied to various devices such as ATMs and door locks in addition to mobile devices. This can be applied to the existing user authentication method using a password.

This study inquired into a password input method using a user's tactile sensation not a password input method depending on vision, which has been mainly re-searched previously. Starting from this study, hopefully, active studies will be carried out on password input methods using various senses of humans.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education

(NRF-2010-0021951)

This work was supported by the BK21 Plus Program (Future-oriented innovative brain raising type) funded by the Ministry of Education(MOE, Korea) and National Research Foundation of Korea(NRF)

REFERENCES

[1] Khan, Muhammad Khurram, Jiashu Zhang, and Xiaomin Wang. "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices." Chaos, Solitons &Fractals Vol.35 No.3 pp.519-524. 2008
[2] Hwang, Min-Shiang, and Li-Hua Li. "A new remote user authentication scheme using smart cards." IEEE Transactions on Consumer Electronics Vol.46, No.1 pp.28-30. 2000
[3] De Luca, A., von Zezschwitz, E., and Hußmann, H. 2009. "Vibrapass: secure authentication based on shared lies". In Procs. of CHI '09. ACM, NY, pp.913-916. 2009
[4] Haller, Neil. "The S/KEY one-time password system.", 1995.
[5] Tomas, J. "Quantifying biometric life insurance risks with non-parametric methods". Diss. Ph. D. thesis, Amsterdam School of Economics Research Institute, 2013.
[6] Bianchi, Andrea, Ian Oakley, and Dong Soo Kwon. "The secure haptic keypad: a tactile password system." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010.
[7] Jansen, Yvonne, Thorsten Karrer, and Jan Borchers. "MudPad: tactile feedback and haptic texture overlay for touch surfaces." ACM International Conference on Interactive Tabletops and Surfaces. ACM, 2010.
[8] Bianchi, Andrea, Ian Oakley, and Dong Soo Kwon. "Spinlock: a single-cue haptic and audio PIN input technique for authentication." Haptic and Audio Interaction Design. Springer Berlin Heidelberg, 2011. 81-90.
[9] Cha, ByungRae, KyungJun Kim, and HyunShik Na. "Random password generation of OTP system using changed location and angle of fingerprint features." Computer and Information Technology, 2008. CIT 2008. 8th IEEE International Conference on. IEEE, 2008.

Yo-Han Choi received the bachelor's degree in the School of Internet Media Engineering from the Korea University of Technology and Education in 2012. He received the MS degree in the Department of Computer Science and Engineering from Korea University of Technology and Education in 2014. Now He is a Ph.D. course student at the Interdisciplinary Program in Creative Engineering from Korea University of Technology and Education, Cheonan, Korea.

His current research interests include mobile Security, Information Security, User Authentication,

Hee-Suk Seo is now a Professor in Department of Computer Science and Engineering, Korea University of Technology and Education, Korea.
His research interests include malicious code analysis, modeling & simulation, network security and intelligent system.

SeungHwan Juis Ph.D. course student in Department of Computer Science and Engineering, Korea University of Technology and Education, Korea.

His current research interests include mobile Security, Information Security, SCADA System Security

SungHyu Hanis now a Professor in School of Liberal Arts, Korea University of Technology and Education, Korea.