Original Article
International Journal of Fuzzy Logic and Intelligent Systems
Vol. 15, No. 4, December 2015, pp. 295-299
http://dx.doi.org/10.5391/IJFIS.2015.15.4.295

ISSN(Print) 1598-2645
ISSN(Online) 2093-744X

Automatic Fortified Password Generator System Using Special Characters

Junho Jeong[1] and Jung-Sook Kim[2]
[1]Department of Computer Science and Engineering, Dongguk University, Seoul, Korea
[2]Division of IT, Kimpo University, Gimpo, Korea

Abstract

The developed security scheme for user authentication, which uses both a password and the various devices, is always open by malicious user. In order to solve that problem, a keystroke dynamics is introduced. A person's keystroke has a unique pattern. That allows the use of keystroke dynamics to authenticate users. However, it has a problem to authenticate users because it has an accuracy problem. And many people use passwords, for which most of them use a simple word such as "password" or numbers such as "1234." Despite people already perceive that a simple password is not secure enough, they still use simple password because it is easy to use and to remember. And they have to use a secure password that includes special characters such as "#!(*)^". In this paper, we propose the automatic fortified password generator system which uses special characters and keystroke feature. At first, the keystroke feature is measured while user key in the password. After that, the feature of user's keystroke is classified. We measure the longest or the shortest interval time as user's keystroke feature. As that result, it is possible to change a simple password to a secure one simply by adding a special character to it according to the classified feature. This system is effective even when the cyber attacker knows the password.

Keywords: Keystroke dynamics, User authentication, Fortified password, Special character, Delayed interval

1. Introduction

A password is used to protect sensitive information and materials. These days, many people have used various passwords due to the development of computers and the Internet. People use a user ID and a password for user authentication on the Internet. The authentication system involves confirming or denying the identity claimed by a person in real-time. Although people use a simple password due to the case of usage and remembrance, it is better for them to use a more secure password that includes special characters such as "#!(*)^" in a password because a simple password is vulnerable to attack from adversary. In order to solve that problem, a biometric based recognition system uses the attributes from physiological (fingerprint, face, iris, etc.) or behavioral (voice, signature, etc.) characteristics of the user himself to perform recognition. But, many biometric techniques require specific tools such as special video cameras to sample the corresponding biometric feature. On the other hand, unlike other biometric methods, keystroke can be done without the aid of additional tools. Because the primary hardware requirement for keystroke biometrics is a keyboard, keystroke biometrics

Received: Dec. 15, 2015
Revised : Dec. 24, 2015
Accepted: Dec. 25, 2015

Correspondence to: Jung-Sook Kim
(kimjs@kimpo. ac.kr)

can be collected from virtually anywhere throughout the world via an Internet connection without requiring an individual to be at certain locations with access to specialized hardware. Keystroke refers to the art and science of recognizing an individual based on an analysis of his typing patterns. Biometric authentication and classification procedures have traditionally been implemented using physiological traits such as fingerprints, retinas, and face, or using behavioral traits such as voice. Typing on a keyboard is already a daily activity for many people; thus, keystroke can be easily integrated into a person's daily routine. Keystroke dynamics verification is based on how the user type in on a keyboard or other generic interfaces equipped with keys, which may belong to a PC, or mobile devices. The keystroke of a person has a unique pattern [1-11]. The relative order in which users press and release keys can vary greatly from user to user, especially while typing words or phrases in which each user has a more established typing pattern. In other words, keystroke dynamics can be used to authenticate the users. For example, when typing the word "the," one user may release may press t, release t, press h, release h, press e, release e, in that order, another user may press all three keys quickly in sequential order before releasing all three keys at the end. Generally, the longest or shortest delayed interval can be measured in same interval position when one person strokes a familiar word on the keyboard. In this paper, we propose the automatic fortified password generator system which uses the keystroke dynamics. At first, the keystroke feature is measured while user key in the password. After that, the feature of user's keystroke is classified. We measure the longest or the shortest interval time as user's keystroke feature. As that result, it is possible to change a simple password to a secure one simply by adding a special character to it according to the classified feature.

The organization of this paper is as follows. Section 2 describes the related works. Section 3 proposes an automatically enhanced password generation system based on keystroke features using special characters. And, in Section 4, we show the experiment results. Finally, conclusions and future work are presented in Section 5.

2. Related Works

The concept of user authentication based on keystroke dynamics (KDA) is not new. The system was proposed by Gaines et al. [1]. It has been the subject of many studies which to improve the text-based KDA system utility [1-5]. Generally it has three phases. In the first phase, the user's keystroke dynamics patterns are stored. In the second phase, the classifier that is applied to a pattern recognition scheme is set up. If the classifier uses a complex algorithm, the user must input the pattern many times. In the last phase, a new classifier input is authenticated.

2.1 Keystroke Features

Four basic keystroke features analyzed previous studies are described as follows [5, 6]. Figure 1 shows that First, Press–Release time, it is the time interval between the stroke for key i^{th} and release of the same key, namely PR(i). Second, Press–Press time, it is the time interval between the stroke for key i^{th} and the stroke for the successive key, namely PP(i). Third, Release–Press time, it is the time interval between the release of key i^{th} and stroke of the successive key, namely RP(i). Finally, Release–Release time, it is the time interval between the release of key i^{th} and the release of the successive key, namely RR(i). It should be noted that the Release-Release time feature can have negative values. Because the key release times do not affect the order of the characters being typed, it is possible for one key to be released before a previous key. Kang et al. [3] proposed a method that generates good-quality input data through artificial rhythms and cues. With good-quality input data, an effective classifier can be generated. Hwang et al. [4] evaluated the effectiveness of keystroke dynamics-based authentication (KDA) on mobile devices. And the use of artificial rhythms to improve authentication performance has been discussed in the paper. Campisi et al. [10] proposed a text-password KDA system that uses a cellular phone keypad. Figure 1 shows four basic keystroke features when a user types in a string "PDAGO"

2.2 Biometrics

Biometrics is the process of uniquely identifying individuals based on one or more physical or behavioral characteristics. Physiological biometrics is related to the shape of the body such as finder print, face, and DNA; while behavioral biometrics is related to the person's behavior such as typing rhythm, gait and signature. The brainwave pattern of every individual is unique and that the EEG can be used for biometric authentication. The uniqueness of EEG signals id particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain on the backside of the head is the best place to measure brainwaves, related to the visual sense. EEG is one of the physiological unique characteristics of an individual. A number

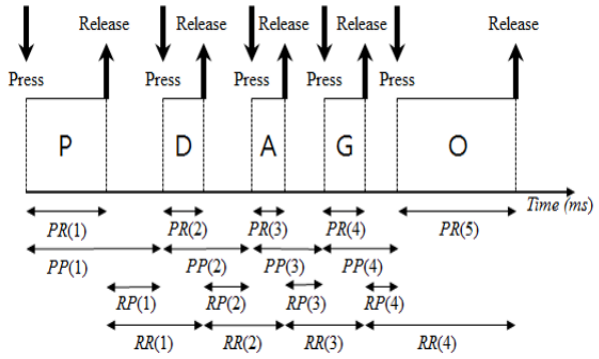

Figure 1. Four basic keystroke features when a user types a string 'PDAGO'. PR, Press-Release time; PP, Press-Press time; RP, Release-Press time; RR, Release-Release time.

of published reports have indicated that there is enough depth in the EEG recording, rendering it suitable as a tool for person authentication. Person authentication aims to accept or to reject a person claiming an identity, i.e. comparing a biometric data to one template. The need of a new behavioral biometric is derived from the need of securing important facilities and important information. Most of the market available secure systems can be penetrated by hacking or by a mistake of one the authorized personnel.

3. Proposed Scheme

The proposed system does not need to authenticate a user how repeat keystrokes, unlike KDA. It makes the user comfortable and facilitates the pattern classification because of the user's characteristics when he or she types in a familiar word are almost concrete. In other words, while typing in a familiar word, there is a high probability that the longest (or shortest) delayed interval will appear in the same position and nearly at the same time. The proposed system has three steps for the fortified password generation. Firstly, the user types in a password and the system records keystroke features of the user. Secondly, the system evaluates the keystroke features that are the longest or shortest delayed interval time comparing the recorded delayed interval time of the keystroke feature. Also, it selects one of the special characters to be inserted into the simple password and decides the distinct section to be added the special character. Finally, it produces the enhanced password instead of the simple password. After that, the new password is saved in a password database. As that result, if your system is attacked by a hacker or malicious user then they could not steal

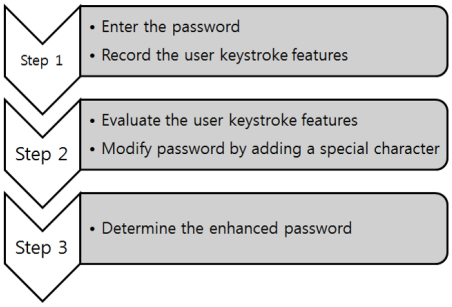

Figure 2. Processing steps.

Table 1. Special characters

Delay time x (ms)	Special character
$0 <= x < 200$	!
$200 <= x < 700$	#
$700 <= x < 1,500$	$
$1,500 <= x < 3,500$	^
$3,500 <= x$	*

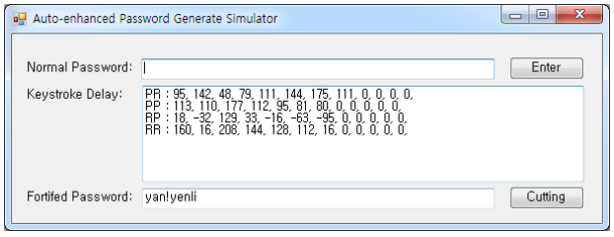

Figure 3. The simulator.

the password. The hacker try to key in a password but he or her has a different keystroke feature. Figure 2 shows the processing steps to generate the enhanced password.

By comparing each interval time of keystroke features a section, where the shortest or longest delay time is the best, can be determined. Then that section is set up as a distinct section. After that, enhanced password can be generated by adding a special character as shown on Table 1 to the distinct section.

4. Experiments and Results

We have implemented a simulator to estimate keystroke features of password such as simple or familiar word and generated an enhanced password. Figure 3 shows a simulator.

The keystroke delay and the automatic fortified password

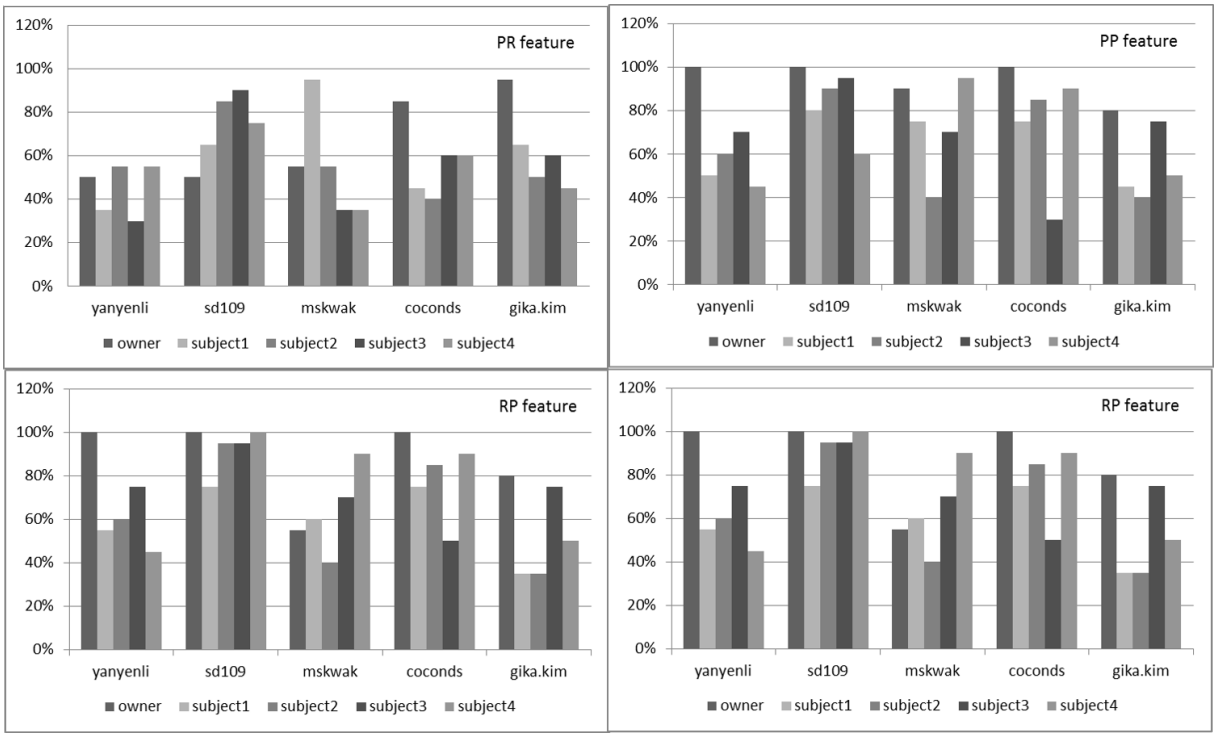

Figure 4. The probability of the same longest delayed interval by keystroke features. PR, Press-Release time; PP, Press-Press time; RP, Release-Press time; RR, Release-Release time.

are displayed in each text box when a user key in a password in the text box. For the experiments, we have determined the subjects and subject's familiar words. The subject typed in a subject's familiar word and that subject typed in the other subject's familiar words on the simulator. Each subject typed in same method. Figure 4 shows the probability of the apperance of the same longest delayed interval by keystroke features of each subjet. The results describe the diffrent probability by keystorke features even during typing in a familiar word. Generally, they show the good case in PP feature. However, in the case of gika.kim, PR feature is good. And in the case of sd109, RP feature bring up a good result. The above results show that the most suitable feature of each case can be different beacuse each user has his/her unique habit or charateristic while they type in a same word.

5. Conclusions and Future Works

A person's keystroke has a unique pattern. That allows the use of keystroke dynamics to authenticate users. However, it has a problem to authenticate users because it has an accuracy problem. And many people use passwords, for which most of them use a simple word such as "password" or numbers such as "1234." Despite people already perceive that a simple password is not secure enough, they still use simple password because it is easy to use and to remember. And they have to use a secure password that includes special characters such as "#!(*)^". In this paper, we propose the automatic fortified password generator system which uses special characters and keystroke feature. Firstly, the user types in a password and the system records keystroke features of the user. Secondly, the system evaluates the keystroke features that are the longest or shortest delayed interval time comparing the recorded delayed interval time of the keystroke feature. Also, it selects one of the special characters to be inserted into the simple password and decides the distinct section to be added the special character. Finally, it produces the enhanced password instead of the simple password. After that, the new password is saved in a password database. As that result, if your system is attacked by a hacker or malicious user then they could not steal the password. The hacker try to key in a password but he or her has a different keystroke feature. This system is effective even when the cyber attacker knows the password. In the future, we will extend this in order to use to the security field.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

References

[1] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results," Rand Corporation, Santa Monica, CA, Report No. RAND-R-2526-NSF, 1980.

[2] M. Obaidat and S. Sadoun, "Verification of a computer user using keystroke dynamics," *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 27, no. 2, pp. 262-269, 1997. http://dx.doi.org/10.1109/3477.558812

[3] P. Kang, S. Park, S. Cho, S. S. Hwang, and H. J. Lee, "The effectiveness of artificial rhythms and cues in keystroke dynamics based user authentication," in *Proceedings of International Workshop on Intelligence and Security Informatics*, Singapore, 2006, pp. 161-162. http://dx.doi.org/10.1007/11734628_22

[4] S. S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Computers & Security*, vol. 28, no. 1, pp. 85-93, 2009. http://dx.doi.org/10.1016/j.cose.2008.10.002

[5] D. Gunetti and C. Picardi, "Keystroke analysis of free text," *ACM Transactions on Information and System Security*, vol. 8, no. 3, pp. 312-347, 2005. http://dx.doi.org/10.1145/1085126.1085129

[6] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351-359, 2000. http://dx.doi.org/10.1016/S0167-739X(99)00059-X

[7] D. Shanmugapriya and G. Padmavathi, "A survey of biometric keystroke dynamics: approaches, security and challenges," *International Journal of Computer Science and Information Security*, vol. 5, no. 1, pp. 115-119, 2009.

[8] S. Hocquet, J. Y. Ramel, and H. Cardot, "User classification for keystroke dynamics authentication," in *Advances in Biometrics*, S. W. Lee and S. Z. Li, Eds. Berlin: Springer, 2007, pp. 531-539. http://dx.doi.org/10.1007/978-3-540-74549-5_56

[9] L. C. Araujo, L. H. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, "User authentication through typing biometrics features," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 851-855, 2005. http://dx.doi.org/10.1109/TSP.2004.839903

[10] P. Campisi, E. Maiorana, M. Lo Bosco, and A. Neri, "User authentication using keystroke dynamics for cellular phones," *IET Signal Processing*, vol. 3, no. 4, pp. 333-341, 2009. http://dx.doi.org/10.1049/iet-spr.2008.0171

[11] J. Jeong and J. S. Kim, "Development of the fortified automatic password generator system," *Advanced Science and Technology Letters*, vol. 58, pp. 63-66, 2014. http://dx.doi.org/10.14257/astl.2014.58.13

Jung-Sook Kim received the B.S., M.S., and Ph.D. degrees in computer engineering from Dongguk University, Seoul, Korea in 1993, 1995 and 1999, respectively. She is a professor in school of Smart IT at Kimpo University. Her research interests include in the fields of intelligent systems, IT convergence, and distributed and parallel system.

Junho Jeong received the B.S., M.S., and Ph.D. degrees in computer engineering from Dongguk University, Seoul, Korea in 2007, 2009 and 2015, respectively. He is a research professor in e-bussiness research center at Dongguk University. His research interests include in the fields of computer security, cloud system and distributed and parallel system.