Advanced Science and Technology Letters
Vol.58 (Security 2014), pp.63-66
http://dx.doi.org/10.14257/astl.2014.58.13

Development of the Fortified Automatic Password Generator System

Junho Jeong[1], Jung-Sook Kim[2]

[1] Dept. of Computer Science and Engineering
Dongguk University, Seoul, Rep. of Korea
[2]Division of IT, Kimpo College, Kimpo, Rep
yanyenli@dongguk.edu, kimjs@kimpo.ac.kr

Abstract. A person's keystroke has a unique pattern. That allows the use of keystroke dynamics to authenticate users. However, it is the problem to authenticate users using the keystroke dynamics due to have an accuracy problem. 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 now secure enough, they still use simple password as it is easy to use and remember. However, they have to use a secure password that includes special characters such as "#!(*)^" for the security reason. Therefore, a Fortified Automatic Password Generator is proposed that uses a longest or shortest delayed interval of each word when people key in a familiar word.

Keywords: Keystroke dynamics, User authentication, Enhanced password

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 authentication on the Internet. 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 "#!(*)^", because a simple password is vulnerable to attack from adversary.

A biometric based recognition system relies on use attributes from physiological (fingerprint, face, iris, etc.) or behavioral (voice, signature, etc.) characteristics of the user himself to perform recognition. 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. 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 [1-4]. In other words, keystroke dynamics can be used to authenticate users. Generally, the most of longest or shortest delayed interval present same interval position when one person strokes a familiar

ISSN: 2287-1233 ASTL

word. Therefore, it is possible to change a simple password to a more secure one simply by adding a special character to it.

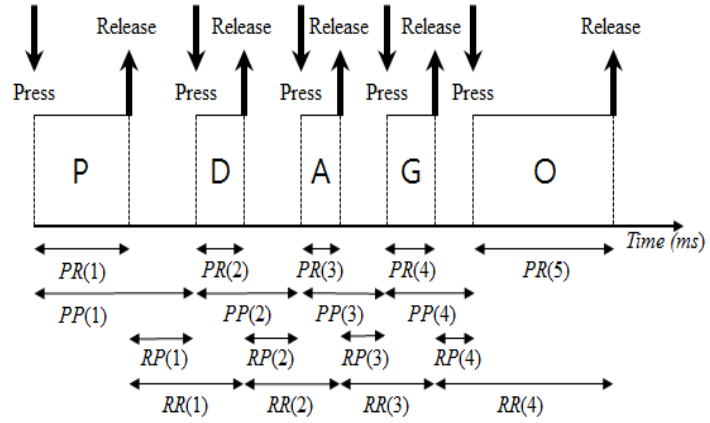

Fig. 1. Four basic keystroke features when a user types a string 'PDAGO'

The organization of this paper is as follows. Section 2 proposes an automatically enhanced password generation system based on keystroke features. And, in Section 3, we show the experiment results. Finally, discussions and conclusions are presented in Section 4.

2 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 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 enhanced password generation. Firstly, the user types in a password and the system records keystroke features of user. Secondly, the system evaluates the keystroke features from the longest or shortest delayed interval from the time of record of the keystroke time. Also, it selects one of the special characters to be inserted into password and the position to be inserted. Finally, the system determines the enhanced password from the entered password.

Table 1. Special character selection

Delay Time x(ms)	Special Character
0 <= x < 200	!
200 <= x < 700	#
700 <= x < 1500	$
1,500 <= x < 3500	^
3,500 <= x	*

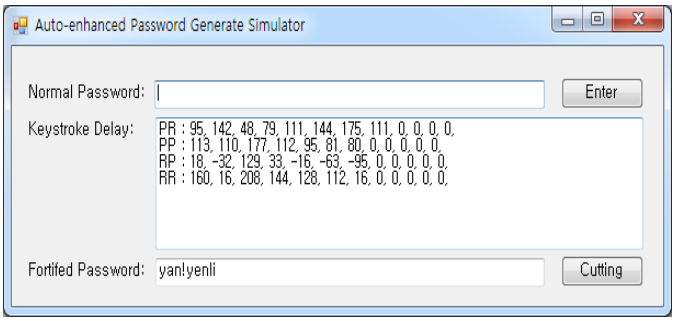

Fig. 2. The simulator

By comparing each interval time of keystroke features, the section where the time gap is the most can be determined. Then this section is set up as distinct section. After that, enhanced password can be generated by adding a special character as shown on table 1to the distinct section.

3 Experiments

We have implemented a simulator to estimate keystroke features of password such as simple or familiar word and generate an enhanced password. Fig.3 shows a simulator. The Keystroke Delay and the Fortified Password display each text box when the password is entered in the text box of Normal Password. Then we have determined subjects and their familiar words. The subject had typed words that included theirs and those of others on the simulator, 20 times for each word.

Fig. 4 show the he probability of the apperance of the same longest delayed interval by keystroke features of subjets. The result describe the diffrence probability by keystorke features even during typing in a familiar word.

Generally, It shows the good case in PP feature. However in the case of giha.kim, PR features and in the case of sd109 RP features bring up a better result. The above result shows, the most suitable feature per case can be different as every user has their unique habit or charateristic while they types in a word.

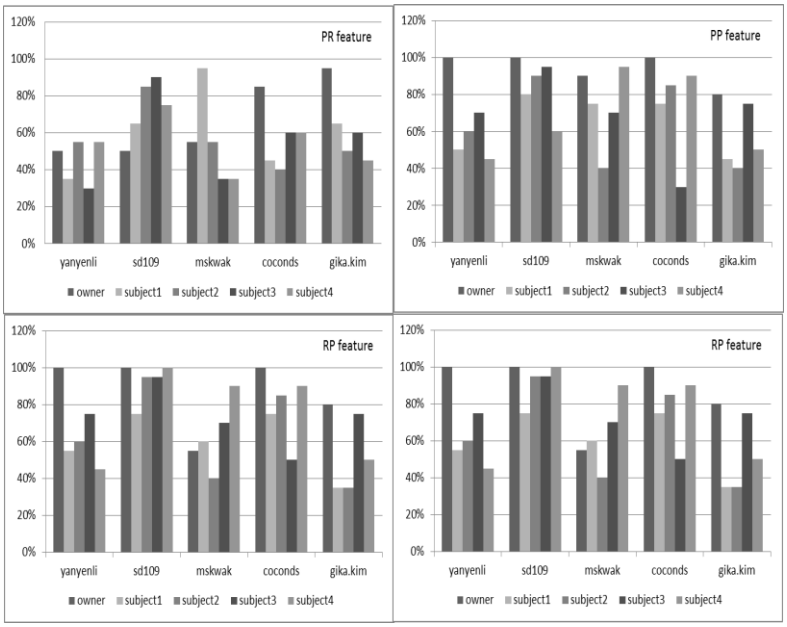

Fig. 3. The probability of the same longest delayed interval by keystroke features

4 Conclusion

The user's characteristics when he or she types in a familiar word as a password were shown. A Fortified Automatic Password Generator was proposed using each word that has the longest or shortest delayed interval when the user types in a familiar word. This system is effective even when the cyber attacker knows the password.

References

1. Gaines, R., Lisowski, W., Press, S. and Shapiro, N.: Authentication by Keystroke Timing: Some Preliminary Results," Rand Report, R-256, NSF, Rand Corp., Santa Monica, CA, (1980)
2. M. Obaidat and S. Sadoum, "Verification of a computer user using keystroke dynamics," In IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics, 27(2), pp. 262-269, (1997)
3. P. Kang, S. Park, S. Cho, S. Hwang and H. Lee, "The Effectiveness of Artificial Rhythms and Cues in Keystroke Dynamics-based User Authentication," In Proceedings of the International Workshop on Intelligence and Security Informatics, pp. 161-162, (2006)
4. S. Hwang, S. Cho, S. Park, "Keystroke dynamics-based authentication for mobile devices," In Computer & Security, 28, pp.85-93. (2009)

