International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 3, June 2018, pp. 1281~1287
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i3.pp1281-1287

The Security Challenges of The Rhythmprint Authentication

Nakinthorn Wongnarukane, Pramote Kuacharoen
Departement of Computer Science, Graduate School of Applied Statistics,
National Institute of Development Administration, Bangkok, Thailand

Article Info

Article history:

Received Dec 28, 2017
Revised Feb 8, 2018
Accepted Mar 13, 2018

Keyword:

Fifth security
First rhythmprint
Fourth biometric
Second multi-touch
Third authentication

ABSTRACT

The Rhythmprint authentication combines an advantage of the traditional keystroke authentication and the multi-touch technology based on a touchable device such as touchpad on a laptop, a smartphone and a tablet. With the Rhythmprint authentication, the user is less likely to suffer from shoulder surfing and eavesdropping attacks. This research provides empirical evidence to verify the security performance of the Rhythmprint authentication comparing to the traditional keystroke authentication for shoulder surfing and eavesdropping attacks, when the user tries to login to a website on a laptop for 10 times in a public place while the attacker stands behind. The experimental results show that the Rhythmprint authentication provides higher security than the traditional keystroke authentication in both shoulder surfing and eavesdropping attacks.

Corresponding Author:

Nakinthorn Wongnarukane,
Departement of Computer Science,
Graduate School of Applied Statistics,
National Institute of Development Administration,
118 Serithai Road, Bangkapi Township, Bangkok 10240, Thailand.
Email: nakinthorn.n@gmail.com

1. INTRODUCTION

The Rhythmprint authentication [1] is a novel method of a biometric authentication. It combines an advantage of the traditional keystroke authentication [2] and the multi-touch technology based on a touchpad on a laptop, a screen of a smartphone and related touchable devices. The Rhythmprint authentication research indicates that the user is less likely to suffer from shoulder surfing and eavesdropping attacks. Furthermore, the initial results show that the Rhythmprint authentication provides higher security than other related methods. This research is looking forward to comparing the security performance of the Rhythmprint authentication to the traditional keystroke authentication, in terms of shoulder surfing and eavesdropping attacks when the user tries to login to an application on laptop in a public place.

The Rhythmprint authentication uses multi-touch technology for collecting the rhythm when the user touches a touchable device. Three measurements which consist of holding time, latency time and number of fingers per beat, are collected and used to create the user template. When the user needs to login to a device, the user only needs to touch fingers on the touchable device with the registered rhythm. K-NN algorithm was used for classification. The attacker must perform shoulder surfing and eavesdropping attacks in order to attack the authentication. This is because the attacker must know two things: the rhythm and the number of fingers per beat. An eavesdropping attack hardly occurs because touching the finger on a device does not makes a loud sound. The algorithm of Rhythmprint authentication can be split into two modules, namely, registration module and authentication module. Figure 1 shows the registraition flowchart of Rhythmprint authentication and Figure 2 shows how authentication of the Rhythmprint authentication works.

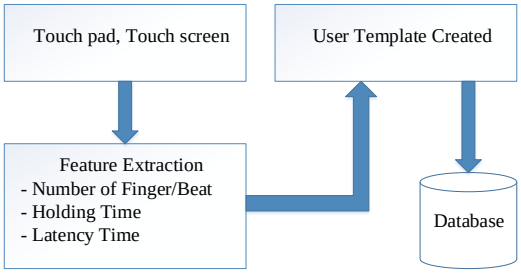

Figure 1. The registration module flowchart

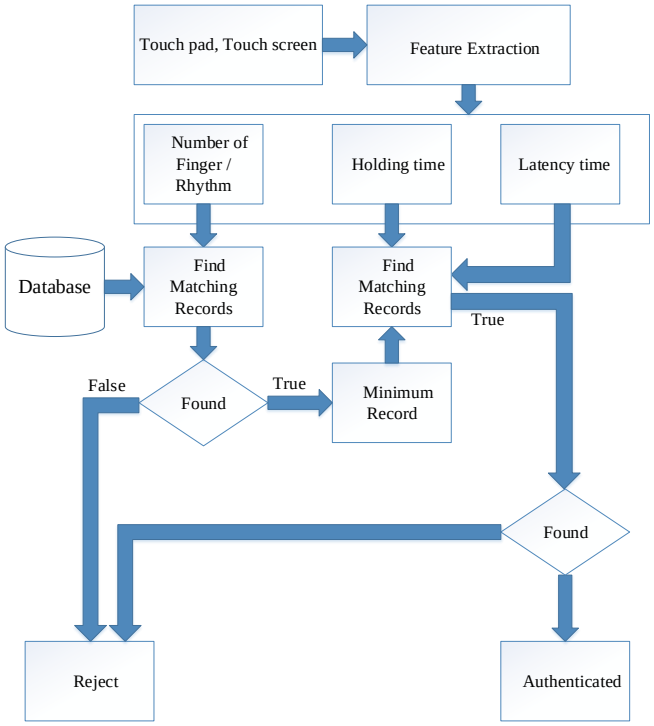

Figure 2. The authentication module flowchart

There are similar studies which use touchable devices to authenticate users. However, these studies have many weak points. PassChords [3] uses multi-touch technology to collect the number of fingers for each tap. Only four tabs are allowed. The user who needs to login to the device must touch four fingers on the screen of smartphone. The system identifies the positions of four fingers including point, middle, ring and little fingers. After that, the phone vibrates and the user can touch on the screen for authentication. PassChords only records the number of fingers per tab, which limits to four taps. Therefore, PassChords is not different from a traditional password authentication. Even worse, PassChords provides weaker security than a password since there are less combinations.

In [4], Keystroke dynamics on android platform was proposed. This is a smartphone authentication by using password that is inputted using softkeys on a smartphone screen. Three measurements which include holding time, latency time and pressing pressure, are used to authenticate users. This method provides better security than using a password alone. However, it is not different from a traditional keystroke dyanamics. It only changes from a hardware keyboard to a virtual keyboard. The pressing pressure is not a suitable factor to use in real life, because the pressing pressure is different when the user is doing different activities.

An extended pin authentication scheme allows multi-touch key input [5] using a PIN and multi-touch technology on smartphones. They allow the user to use more than one finger when touching digit buttons on the screen. It is similar to the work in [4] but the scheme only uses a numeric virtual keyboard and adds multi-touch for keyboard input.

Development of a typing behavior recognition mechanism on Android and traditional keystroke [6] is just like a tradition keystroke, but it moves from hardware keyboard to smartphone screen, using three measurements: holding time, latency time and password.

The proposed methods in [4]-[6] have the same weak point, the user must look at the screen until the authentication is successful. Because the method uses a virtual keyboard and the screen is small, if the user is not looking on the screen while tapping, the user will not be able to login successfully. This method also suffers from shoulder surfing attacks. For the proposed method in [3], the user does not need to look at the screen when loging in, unlike [4]-[6]. However, in public places, using only the number of fingers per tap as an authentication is not enough to prevent shoulder surfing attacks. When comparing only functions of the Rhythmprint authentication with [2]-[6], we found that the Rhythmprint authentication provides higher security than others methods.

In this paper, we provide an empirical assessment of the security performance of the Rhythmprint authentication in terms of shoulder surfing and eavesdropping attacks. The results of experiments are compared with the traditional keystroke authentication.

2. RESEARCH METHOD

This research attempts to measure the Rhythmprint authentication [1] security in terms of shoulder surfing and eavesdropping attacks by comparing to a traditional keystroke authentication. We implemented all authentication programs for the Rhythmprint authentication and the traditional keystroke methods on laptops. For the experimental design, we simulate the situation where the user must authenticate himself/herself to an application on a laptop while sitting in a public place and an attacker stands behind the user. The attacker stands behind the user all the time while the user is trying to authenticate himself/herself to application on a laptop using the Rhythmprint authentication and the traditional keystroke authentication.

For each method, the user must try to authenticate 10 times, the attacker has to perform shoulder surfing and eavesdropping attacks everytime. The user enters the password on the keyboard for the traditional keystroke authentication and makes the rhythm on the touchpad for the Rythmpring authentication. Everytime the user can authenticate successfully, we test whether or not the attacker is able to authenticate on the victim's laptop. The results are recorded. Figure 3 shows the simulated situation of shoulder surfing attacks. We design the experiment using two methods including with a hand covering and no hands covering as described in detail in the following sections.

Figure 3. The shoulder surfing attack situation

2.1. Hand covering

We allow the user to use the other hand to cover the touching hand when tapping on the touchpad or stroking the keyboard. Figure 4 shows when the user tries to authenticate to the applicaiton on a laptop with the traditional keystroke method with hand covering and Figure 5 shows when the user tries to authenticate to the applicaiton on a laptop with the Rhthmprint method and uses the hand to cover.

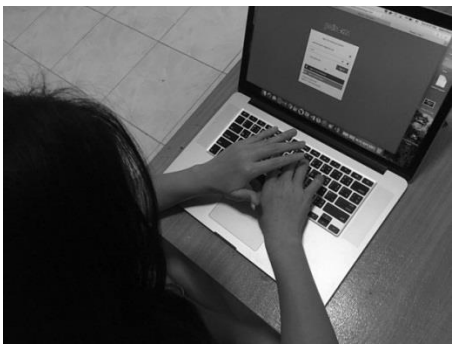

Figure 4. The traditional keystroke authentication with hand covering

Figure 5. The Rhythmprint authentication with hand covering

2.2. No hand covering

We do not allow the user to use the other hand to cover the touching hand when tapping on the touchpad or stroking the keyboard. Figure 6 shows when the user tries to authenticate to the applicaiton on a laptop with the traditional keystroke method without hand covering and Figure 7 shows when the user tries to authenticate to the applicaiton on a laptop with the Rhthmprint method without hand covering.

Figure 6. The traditional keystroke without hand covering authentication

Figure 7. The Rhythmprint without hand covering authentication

3. RESULTS AND ANALYSIS

For verifying our proposed method, we designed and developed software on a laptop uisng Java programming language. For a laptop in our experiment, we used Macbook Pro by Apple Inc. We recruited 10 participants which consists of five males and five females, between 30-40 and one male as an attacker.

All users must authenticate themselves to the application on our laptop 10 times per method, while the attacker is standing behind them. Each time the authentication is complete, the attacker tries to authenticate himself on the victim's laptop. The experiment is divided into two parts including hand covering and no hands covering experiments.

3.1. Hand covering experimental results

While users were tapping on the screen or stroking the keyboard to authenticate themselves, we allowed users to use the other hand to cover the tapping hand. Table 1 shows the experimental results of this method.

From Table 1, we can calculate the security performance of the Rhythmprint method comparing to the traditional keystroke method by using arithmetic mean ($\bar{x}$) and S.D. (standard deviation).

The equation of $\bar{x}$ is shown below

$$\frac{x1 + x2 + x3 + \cdots + xn}{n}$$

The equation of S.D. is shown below

$$\text{S. D.} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n}}$$

$\bar{x}$ of the Rhythmprint is

$$\frac{0+0+0+9+0+0+0+8+0+0}{10} = 1.7$$

S.D. of the Rhythmprint is

$$S.D._{Rhythmprint} = \sqrt{\frac{\begin{matrix}(0-1.7)^2+(0-1.7)^2+(0-1.7)^2+(9-1.7)^2+\\(0-1.7)^2+(0-1.7)^2+(0-1.7)^2+(8-1.7)^2+\\(0-1.7)^2+(0-1.7)^2\end{matrix}}{10}} = 3.41$$

$\bar{x}$ of the traditional keystroke is

$$\frac{7+0+8+9+0+5+7+9+9+0}{10} = 5.4$$

S.D. of the traditional keystroke is

$$S.D._{Rhythmprint} = \sqrt{\frac{\begin{matrix}(7-5.4)^2+(0-5.4)^2+(8-5.4)^2+(9-5.4)^2+\\(0-5.4)^2+(5-5.4)^2+(7-5.4)^2+(9-5.4)^2+\\(9-5.4)^2+(0-5.4)^2\end{matrix}}{10}} = 3.72$$

Table 1. Hand Cover Experimental Results

User	Attack Success Time	
	Rhythmprint	Keystroke
1	0	7
2	0	0
3	0	8
4	9	9
5	0	0
6	0	5
7	0	7
8	8	9
9	0	9
10	0	0

3.2. No hand covering experimental results

While users were tapping on the screen or stroking the keyboard to authenticate themselves, users were not allowed to use the other hand to cover the tapping or the typing hand. Table 2 shows the experimental results of this method.

From Table 2, we can calculate the security performance of Rhythmprint method comparing to the traditional keystroke method by using arithmetic mean ($\bar{x}$) and S.D. (standard deviation).

$\bar{x}$ of the Rhythmprint is

$$\frac{0+8+0+0+7+0+7+0+9+0}{10} = 3.1$$

S.D. of the Rhythmprint is

$$S.D._{Rhythmprint} = \sqrt{\frac{\begin{matrix}(0-3.1)^2+(8-3.1)^2+(0-3.1)^2+(0-3.1)^2+\\(7-3.1)^2+(0-3.1)^2+(7-3.1)^2+(0-3.1)^2+\\(9-3.1)^2+(0-3.1)^2\end{matrix}}{10}} = 3.83$$

$\bar{x}$ of the traditional keystroke is

$$\frac{3+5+4+2+4+3+5+1+7+8}{10} = 4.2$$

S.D. of the traditional keystroke is

$$S.D_{\cdot Rhythmprint} = \sqrt{\frac{\begin{matrix}(3-4.2)^2+(5-4.2)^2+(4-4.2)^2+(2-4.2)^2+\\(4-4.2)^2+(3-4.2)^2+(5-4.2)^2+(1-4.2)^2+\\(7-4.2)^2+(8-4.2)^2\end{matrix}}{10}} = 2.04$$

The experimetal results show the security performance of the Rhythmprint authentication comparing to the traditional keystroke authentication. In the hand covering method case, only 2 of 10 volunteers of the Rhythmprint authentication were attacked successfully and the minimum time to crack the victim's rhythm is 8, but 7 of 10 of the traditional keystroke authentions were attacked and the minimum time to crack victim's stroke is 5. The $\bar{x}$ and S.D. of the experiment in this case show that the Rhythmprint authentication provides higher security than traditional keystroke. In the no hand covering method case, only 4 of 10 volunteers of the Rhythmprint authentication were attacked successfully and the minimum time to crack victim's rhythm is 7, while all of the traditional keystroke authentications were attacked and the minimum time to crack victim stroke is 1. The $\bar{x}$ and S.D. of the experiment in this case show that the Rhythmprint authentication also provides higher security than the traditional keystroke.

Table 2. No. Hand Cover Experimental Results

User	Attack Success Time	
	Rhythmprint	Keystrike
1	0	3
2	8	5
3	0	4
4	0	2
5	7	4
6	0	3
7	7	5
8	0	1
9	9	7
10	0	8

4. CONCLUSION

From the experimeatal results, we can conclude the Rhythmprint authentication provides higher security than the traditional keystroke authentication in terms of shoulder surfing and eavesdropping attacks. For the Rhythmprint authentication, when the user touches or tabs on the touchpad, it does not make a loud sound. Therefore, eavesdropping attacks is unlikely. However, the traditional keystroke authentication can suffer from eavesdropping attacks if the user is not careful when typing on the buttons.

For the shoulder surfing attacks, since the Rhythmprint authentication does not require any button and any fixed position on the touchpad, the user can touch the finger on the touchpad without looking at the touchpad and can use the other hand to cover while touching. However, the traditional keystroke authentication requires the buttons which are located at fixed positions. As a result, the user must be able to see keyboard while making strokes for authentication. If the user uses the other hand to cover the stroking hand, the user can perform the task more slowly which can be easily detected by an attacker. The experiment shows that if the users tried to authenticate in a public place without anything covering the stroking hand in the traditional keystroke authentication, the users were attacked 100% of the time. However, only 4 of 10 volunteers of the Rhythmprint authentication were attacked successfully and the minimum time to crack a victim rhythm is 7.

REFERENCES

[1] N. Wongnarukane and P. Kuacharoen, "Rhythm Authentication Using Multi-touch Technology: A New Method of Biometric Authentication," *Lecture Notes in Computer Science (LNCS) Springer, Cham.*, 2017, pp. 390-399.
[2] D. Shanmugapriya and P. Ganapathi, "A survey of biometric keystroke dynamics: Approaches, security and challenges," *arXiv preprint* arXiv:0910.0817, 2009.
[3] S. Azenkot, *et al.*, "PassChords: secure multi-touch authentication for blind people," in *Proc. of the 14th international ACM SIGACCESS conference on Computers and accessibility*, Oct 2012.

[4] M. Antal, Z.S. László and L. Izabella, "Keystroke dynamics on android platform," *in Procedia Technology*, 2015.
[5] T. Takada and Y. Kokubun, "Extended pin authentication scheme allowing multi-touch key input," in *Proc. of International Conference on Advances in Mobile Computing & Multimedia*, Dec 2013.
[6] X. Huang, G. Lund and A. Sapeluk, "Development of a typing behaviour recognition mechanism on Android", In *2012 IEEE 11th International Conference on Trust, Security and Pri-vacy in Computing and Communications, IEEE*, Jun 2012.

BIOGRAPHIES OF AUTHORS

Nakinthorn Wongnarukane. Received his B.S. in computer science from Kasetsart University and M.E. degrees in computer science from National Institute of Development Administration (NIDA) in 2010 and 2012. He started studying in Ph.D. in 2015 at National Institute of Development Administration in computer science. His research interests are information security and mobile application.

Assistant Professor Dr. Pramote Kuacharoen. Received his B.S. and M.E. degrees in computer and systems engineering from Rensselaer Polytechnic Institute (RPI) in 1995 and 1996, respectively. He also received his M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology in 2001 and 2004, respectively. He joined the Department of Computer Science at National Institute of Development Administration in 2004. His research interests include computer and network security, information security, computer networks, embedded systems, and mobile applications design and development.