Authentication with Time Features for Keystroke Dynamics on Touchscreens

Matthias Trojahn[1], Florian Arndt[1], and Frank Ortmeier[2]

[1] Volkswagen AG, Wolfsburg, Germany
[2] Otto-von-Guericke University of Magdeburg, Computer Systems in Engineering, Magdeburg, Germany
{matthias.trojahn,florian.arndt1}@volkswagen.de,
frank.ortmeier@ovgu.de

Abstract. Keystroke authentication is a well known method to secure the mobile devices. Especially, the increasing amount of personal and sensitive data stored on these devices makes a secure authentication system necessary. Traditional security techniques like the four-digit PIN-input are insufficient and do not correspond to the present password standards. A keystroke behavior based authentication system could increase the security. Different researches have been published based on keystroke authentication systems with traditional PC keypads. But the keystroke behavior on touchscreens, as they are nowadays used on smartphones, are not analysed before.

Keywords: keystroke authentication, mobile devices, capacitive display.

1 Introduction

Today, smartphones are not only used like normal telephones to phone or write SMS's. This changed with the introduction of the iPhone in the year 2007. With this or other smartphones the number of security relevant data and information which are stored on the smartphone (or provided through applications) are increased.

Different studies showed already an improvement for the authentication if keystroke dynamics are used [1,2]. But the existing publications are mainly dealing with computer keyboards or 12-key hardware keyboard of mobile phones.

In this paper, we will discuss the standard features of keystroke dynamics on touchscreen devices. The goal is to see that an authentication with a touchscreen keyboard can be done. On the following questions our research is focused. If an authentication is done with a touchscreen keyboard using time features, the same error rates can be achieved compared with the existing keystroke dynamics studies.

2 Keystroke Authentication Background

Keystroke behaviour can be described as a biometric characteristic of a person. In particular how this person is typing on a keyboard [3]. It is used like other

B. De Decker et al. (Eds.): CMS 2013, LNCS 8099, pp. 197–199, 2013.

biometric methods to verify a person. Furthermore, the rhythm how a person is typing can be calculated by different points but at least the time differences are used [4].

In general, two basic types of events can be recorded: The duration time which describes how long a key is pressed (time between pressing and releasing a key) is the first type. The second one describes the time period between n keystrokes, defined by the n press events. This is called n-graph [4]. Several variants of the time period exist. The most used is the digraph were n=2. In addition, some publications are using the combination of three key presses. This is called the trigraph [5]. Basically, each value over n $>$ 1 is possible in order to determine the time differences. But with a higher value the information decreases which can be extracted by the input. The reason with a higher value is that an average over n events is calculated.

3 Experimental Design and First Results

In our experiment, the subjects were asked to enter a predefined, 17-digit pass phrase on a smartphone (ten times in a row). For the experiment we used a Samsung Galaxy Nexus. To record the information of the keyboard we implemented a soft keyboard, in addition, to an application were the subject had to type the pass phrase.

As a first evaluation we calculated the standard features (duration time of the keystroke, the digraph and trigraph). Figure 1 shows the extracted data for five randomly selected subjects (like [6,7]). The left figure shows the data of the digraph and while the right represents the data of the duration time.

On the left, it can be seen that the average duration is in most cases more constant over the time. However, there are differences between the people. Even the general speed or the time between single digraphs of one subject differs. The differences between one subject can be explained on the basis of experience. E.g. the fifth person has a lot of experience while subject number four has no experience. This is the reason why the fourth person has a higher value for each

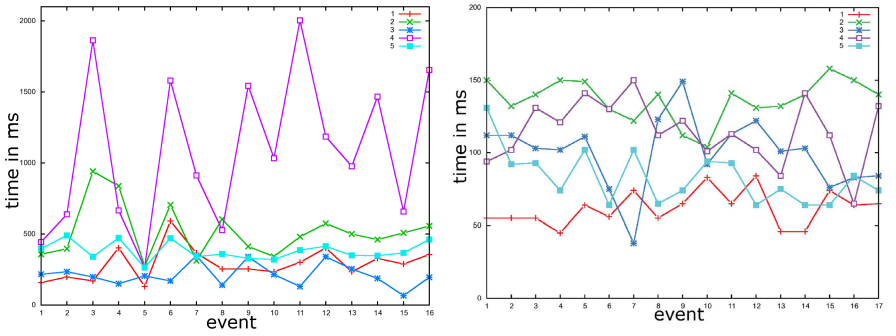

Fig. 1. (left) Digraph for five different users, (right) duration time of the same subjects

digraph than the others. The small value for the digraph at fifth time event for all subjects can be explained by a double letter in the pass phrase. No subject has to search the next letter in this situation.

The rhythm of the duration time (Figure 1 on the right), is less constant between individuals and, in addition, between different attempts by one person. Furthermore, the duration time tends to be less than the digraph. A person needs more time to press the next key than to hold a key.

4 Conclusion

The first result of this experiment shows that there are inter-differences between subjects for the time features and intra-similarities between different attempts of one user. This has to be evaluated more in a bigger experiment. On touchscreen keyboards, which are now installed in nearly every smartphone, besides the well-known features, other possibilities for typing behavior can be recorded. Examples for this are the pressure or the size of the fingertip during typing. These can be used in combination with the time values for authentication [8].

References

1. Joyce, R., Gupta, G.: Identity authentication based on keystroke latencies. Commun. ACM 33, 168–176 (1990)
2. Ord, T., Furnell, S.: User authentication for keypad-based devices using keystroke analysis. In: Proc. 2nd Int'l Network Conf. (INC 2000), pp. 263–272 (2000)
3. Monrose, F., Rubin, A.D.: Authentication via keystroke dynamics. In: Proceedings of the 4th ACM Conf. on Computer and Communications Security, CCS 1997, pp. 48–56. ACM, New York (1997)
4. Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Löhlein, B., Heister, U., Möller, S., Rokach, L., Elovici, Y.: Identity theft, computers and behavioral biometrics. In: Proceedings of the 2009 IEEE Intl. Conf. on Intelligence and Security Informatics, ISI 2009, pp. 155–160. IEEE Press, Piscataway (2009)
5. Chorąś, M., Mroczkowski, P.: Keystroke dynamics for biometrics identification. In: Beliczynski, B., Dzielinski, A., Iwanowski, M., Ribeiro, B. (eds.) ICANNGA 2007, Part II. LNCS, vol. 4432, pp. 424–431. Springer, Heidelberg (2007)
6. Lau, E., Liu, X., Xiao, C., Yu, X.: Enhanced user authentication through keystroke biometrics. In: Computer and Network Security (2004)
7. Clarke, N.L., Furnell, S.M.: Authenticating mobile phone users using keystroke analysis. Int. J. Inf. Sec., 1–14 (2006)
8. Ross, A., Jain, A.K.: Information fusion in biometrics. Pattern Recognition Letters 24, 2115–2125 (2003)