Keystroke Authentication on Mobile Devices with a Capacitive Display

Matthias Trojahn[1] and Frank Ortmeier[2]
[1] *Volkswagen AG, Wolfsburg, Germany*
[2] *Computer Systems in Engineering, Otto-von-Guericke University, Magdeburg, Germany*

Keywords: Security, Keystroke Authentication, Pressure, Mobile Devices, Capacitive Display.

Abstract: Nowadays, it is common to address security problems in the newspaper. Losing or stealing of mobile devices (smartphones and tablets) is in particular an important topic. A lot of information can be stored and accessed via these devices. The one reason why this problem exists, is because the mobile devices are not secured properly. In our work we present an authentication method for these mobile devices.We are using the keystroke dynamics during typing a PIN (four or six numbers) or password. With this the security of the devices gets improved. Keystroke dynamics are already used for authentication on PCs and on mobile phones with hardware keys on a 12-key layout.

1 INTRODUCTION

Biometric user authentication (something-you-are) is an established authentication method beside the something-you-know (PIN and password) and the something- you-have factor (smart card or one-time-password). The advantage with biometric methods is that this factor cannot be stolen or lost like smart cards. The user himself is the factor. Two groups of biometric authentication methods are known. One is the passive methods (e.g. fingerprint or face recognition), the other are active or behavior methods like voice or signature recognition. One disadvantage is that biometric authentication is differing each time (Ross et al., 2006). These changes can occur because of different aspects (e.g. temporary illnesses or especially behavior methods have every time small differences).

That is why two different error rates are known. These are called FAR (False Acceptance Rate) and FRR (False Rejection Rate). FAR describes the percentage between the false accepted people divided by all authentication attempts (Vielhauer, 2006). FRR defines how much people cannot authenticate himself even if they are the person how they claim to be (Vielhauer, 2006). Both rates are used to compare authentication methods.

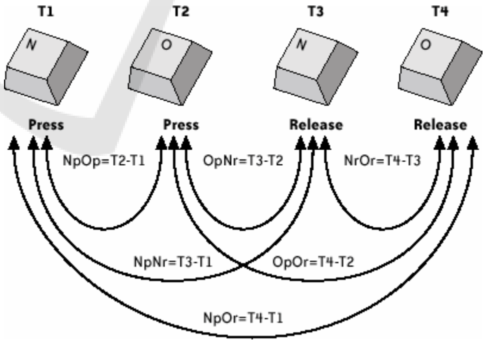

Figure 1: Digraph between letter N and O (e.g. time between pressing and releasing one key or time(Cranor and Garfinkel, 2005).

2 BACKGROUND

The authentication via keystroke dynamics started with first studies for the keyboard of computer. Today, some companies are already selling keystroke authentication with a special keyboard. Important for each method is to choose a good set of features and classifiers. Well known features for keystroke are the digraph (time between two events - see Figure 1) (Maiorana et al., 2011) and the error rate (times the user erases a letter) (Buchoux and Clarke, 2008).

The research of Monrose et al. (Monrose and Rubin, 2000) where they used a Bayesian classifier showed good results with an accuracy of around 92,1% which represents EER of 7,9%. These meth-

Trojahn M. and Ortmeier F..
Keystroke Authentication on Mobile Devices with a Capacitive Display.
DOI: 10.5220/0004344806370640
In *Proceedings of the 2nd International Conference on Pattern Recognition Applications and Methods* (BTSA-2013), pages 637-640
ISBN: 978-989-8565-41-9

ods were adapted to the mobile phones with a 12-key layout with physical keys by different researches (Clarke and Furnell, 2006; Maiorana et al., 2011). Common classifiers are neural networks, Bayesian classifier or stastistical classifier (Alsulaiman et al., 2008; Monrose and Rubin, 2000). With these the error rates were lowered over the years and today FAR and FRR can be lower than 5% (as described in the survey of Shanmugapriya (Shanmugapriya and Padmavathi, 2009)). Because of the technology changes in the last years smartphones use a different input method. The physical keys are replaced by a capacitive display and no 12-key layout is used anymore. Instead, we are using a full featured QWERTY-layout.

3 KEYSTROKE USING THE CAPACITIVE DISPLAY

A new layout creates different challenges. Limited physical feedback and smaller keys will lead to not so good results during authentication (Trojahn and Ortmeier, 2012). The capacitive display can give a feedback with a vibration signal but like before it is not possible to recognize whether one key was pressed in the middle or at the edge. Previously, it was possible for the user to recognize if two keys were pressed at the same time. To compensate these challenges new features have to be added to the authentication process. In addition, different features could be added to the digraph (time between two events) and error count:

- phyisical pressure during typing of the fingertip
- size of the fingertip which is pressing on the device researchs
- exact location (X/Y-coordinates)
- angle in which the user holds the device

In other researchs (Luca et al., 2012) pressure and size were used but only for a 3x3 point matrix where the user had to draw a figure connecting these points. The FAR in this scenario was 21% and the FRR was 19%.

4 EXPERIMENT

A first experiment with 18 user allowed to obtain preliminary results for an keystroke authentication with a capacitive display. In Figure 2 first differences are shown with the digraph and the pressure during typing. Five samples of different user are shown in the figures which shows the differences between the user.

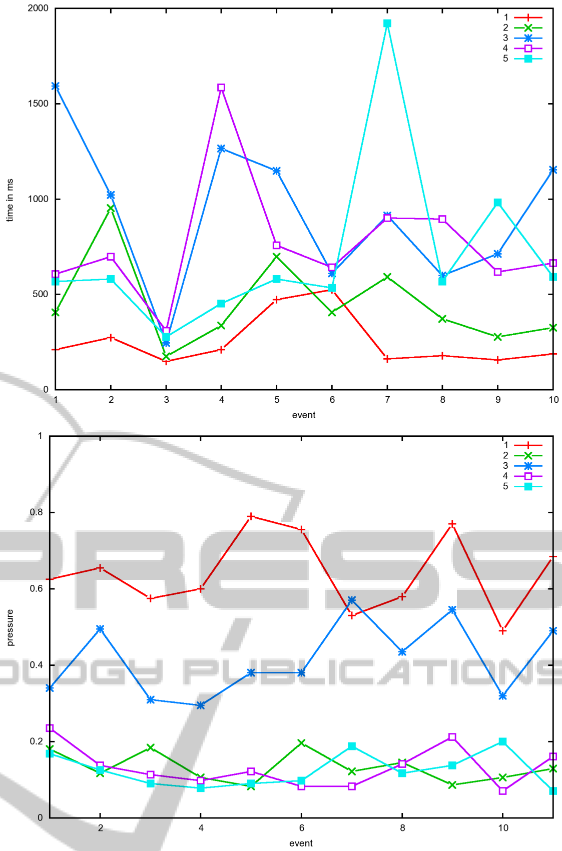

Figure 2: (top) digraph of five user; (bottom) pressure during typing (same users).

11 letters had to be written by each user ten times. The third and fourth were the same so the digraph for the difference is smaller than the most of the rest of the digraphs.

This experiment had a FAR of 2% and a FRR of 2.7% with an J48 classifier (using the weka environment (Hall et al., 2009)). Additional tests with other classifier (neuronal networks or baysian classifier) showed that both fault error rates are under 10%. The result for a statistical classification algorithm (cluster analysis) was that for this set of user the FAR and FRR is lower than 1%. During the enrollment seven samples were used for creating the model of a person where the two outlier values were extracted as error extraction. The other three samples were used for the evaluation of this method using the distance measure.

5 DISCUSSION

In addition, several different scenarios exist which can influence the input behavior of a person and can result

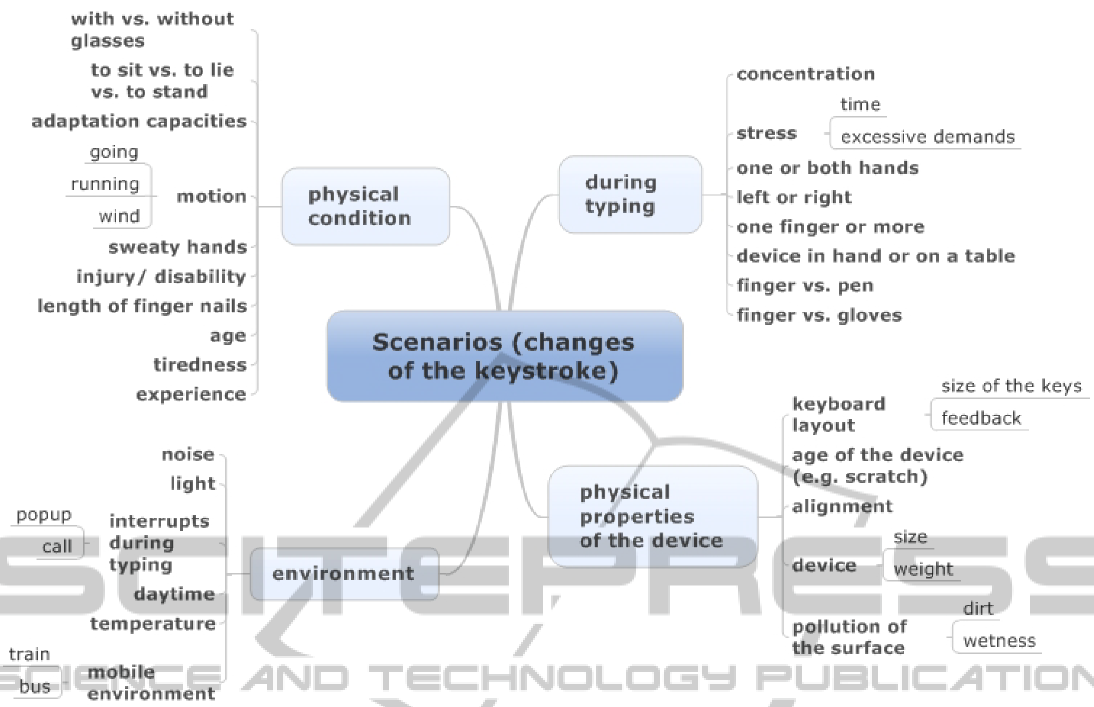

Figure 3: Different scenarios for changing the input behavior.

to a rejection. Some of these scenarios are shown in Figure 3. These have to be tested whether they influence the keystroke behavior or not.

Some scenarios are the result of physical changes of the device and other are influenced by the environment. In the darkness or if the light is glaring, the user may not see the keys really good. This can result in a slower input behavior than normal (Fitts, 1992; Funk et al., 2012).

Furthermore, physical conditions are important. Especially, if the user is in motion e.g. going or running somewhere (Owens, 1984) or whether the user is tired (Pan et al., 1994). In some situation a person has time pressure during typing (stress) which influence the behavior (Vizer et al., 2009).

6 CONCLUSIONS AND FUTURE WORK

The first results show that an authentication with this method on smartphones is possible. In the future, more experimental tests have to be done with more people. In addition, it has to be tested how the keystroke dynamic is affected by stress, for example time pressure and other scenarios which were presented. Moreover, possible attacks have to be tested to show the security and robustness of this method. With the usage of neuronal networks a solution have to be generated how negative examples are created in a real scenario to train the neuronal network. In test case negative examples are generated by other user when they using the same password. In a real scenario the password should be unique that means no negative examples exists.

Also other forms of input methods are possible. One is to use the swype *(www.swype.com)* method where the user has a normal keyboard on the touch pad. There the user is drawing / swyping a continuous line where the user starts at the first letter and is drawing a line to the next letter and so on. One word is represented by one line.

REFERENCES

Alsulaiman, F. A., Cha, J., and Saddik, A. (2008). User identification based on handwritten signatures with haptic information. In *Proceedings of the 6th international conference on Haptics: Perception, Devices and Scenarios*, EuroHaptics '08, pages 114–121, Berlin and Heidelberg. Springer-Verlag.

Buchoux, A. and Clarke, N. L. (2008). Deployment of keystroke analysis on a smartphone. In *Proceedings of the 6th Australian Information Security & Management Conference*.

Clarke, N. L. and Furnell, S. M. (2006). Authenticating mobile phone users using keystroke analysis. In *Int. J. Inf.*

Secur, volume 6, pages 1–14, Berlin and Heidelberg. Springer-Verlag.

Cranor, L. F. and Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, illustrated edition.

Fitts, P. M. (1992). The information capacity of the human motor system in controlling the amplitude of movement. 1954. *J EXP PSYCHOL GEN*, 121(3):262–269.

Funk, R. E., Taylor, M. L., Creekmur, C. C., Ohlinger, C. M., Cox, R. H., and Berg, W. P. (2012). Effect of walking speed on typing performance using an active workstation 1,2. *Perceptual and Motor Skills*, 115(1):309–318.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., and Witten, I. H. (2009). The weka data mining software: An update. In *SIGKDD Explorations*, volume 11.

Luca, A. d., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. (2012). Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *CHI'12*, pages 987–996.

Maiorana, E., Campisi, P., González-Carballo, N., and Neri, A. (2011). Keystroke dynamics authentication for mobile phones. In *Proceedings of the 2011 ACM Symposium on Applied Computing*, SAC '11, pages 21–26, New York and NY and USA. ACM.

Monrose, F. and Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. In *Future Generation Computer Systems*, volume 16, pages 351–359. Elsevier Science Publishers B. V.

Owens, D. A. (1984). The resting state of the eyes: Our ability to see under adverse conditions depends on the involuntary focus and convergence of our eyes at rest. In Sigma Xi, T. S. R. S., editor, *American Scientist*, pages 378–387.

Pan, C. S., Shell, R. L., and Schleifer, L. M. (1994). Performance variability as an indicator of fatigue and boredom effects in a vdt data–entry task. *International Journal of Human-Computer Interaction*, 6(1):37–45.

Ross, A. A., Nandakumar, K., and Jain, A. K. (2006). *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag New York, Inc, Secaucus and NJ and USA.

Shanmugapriya, D. and Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges. In *International Journal of Computer Science and Information Security*, volume abs/0910.0817 of *Vol. 5, No. 1*.

Trojahn, M. and Ortmeier, F. (2012). Biometric authentication through a virtual keyboard for smartphones. In *International Journal of Computer Science & Information Technology (IJCSIT)*.

Vielhauer, C. (2006). *Biometric User Authentication for IT Security: From Fundamentals to Handwriting*. Advances in information security. Springer-Verlag.

Vizer, L. M., Zhou, L., and Sears, A. (2009). Automated stress detection using keystroke and linguistic features: An exploratory study. *International Journal of Human-Computer Studies*, 67(10):870–886.