BIOMETRIC AUTHENTICATION THROUGH A VIRTUAL KEYBOARD FOR SMARTPHONES

Matthias Trojahn[1]andFrank Ortmeier[2]

[1]Volkswagen AG, Wolfsburg, Germany
matthias.trojahn@volkswagen.de
[2]Otto-von-Guericke University, Magdeburg, Germany
frank.ortmeier@ovgu.de

ABSTRACT

Security through biometric keystroke authentication on mobile phones with a capacitive display and a QWERTZ-layout is a new approach. Keystroke on mobile phones with a 12-key layout has already shown the possibility for authentication on these devices. But with hardware changes, new general requirements have been arisen.

In this paper, we focus on the authentication with keystroke dynamics. Therefore, we are presenting new implemented keyboard layouts to show differences between a 12-key layout and a QWERTZ-layout. In addition, we compare a numerical (PIN) and alphabetic (password) input for mobile phones. For this, we added new features for a keystroke authentication with a capacitive display. With the knowledge of the fault rates, we discuss the improvement of the security for keystroke dynamics with different virtual keyboard layouts. Our results show, even with new hardware factors, that an authentication via keystroke dynamics is possible.

KEYWORDS

Authentication, biometrics, keystroke, smartphone, virtual keyboard

1. INTRODUCTION

In 2008, a survey from Credant Technologies reported that in six months 3,000 laptops and 55,000 cellular phones were left in London taxis [1].

The loss and steal of devices is getting a big problem because the data are not secured properly. In big companies, computers are secured with a two-factor authentication. Most authentication methods are not suitable for tablets or smartphones but these devices are basically a small computer because of all their storage and processor power. All the data and application can be accessed with only a pin or password. These methods are insecure because most passwords are to short or to easy (20% of the users are using 5000 of the most popular passwords [2]). Even for passwords with a properly length and alphanumeric letters which are not in the dictionary, other methods like social engineering [3] and Keylogger [4] can be used to steal the password.

A lot of methods have been developed or improved in the last years. Milestones like the introduction of the first iPhone[5] changed the main usage of mobile devices. Not only phone calls are done or SMS are written anymore; many interactions can be done, like surfing in the Internet. In addition, the input method has changed at this time. Hardware keyboards with 12 keys are replaced by a capacitive display with a full featured QWERTZ-layout keyboard (see Figure 1).

DOI : 10.5121/ijcsit.2012.4501

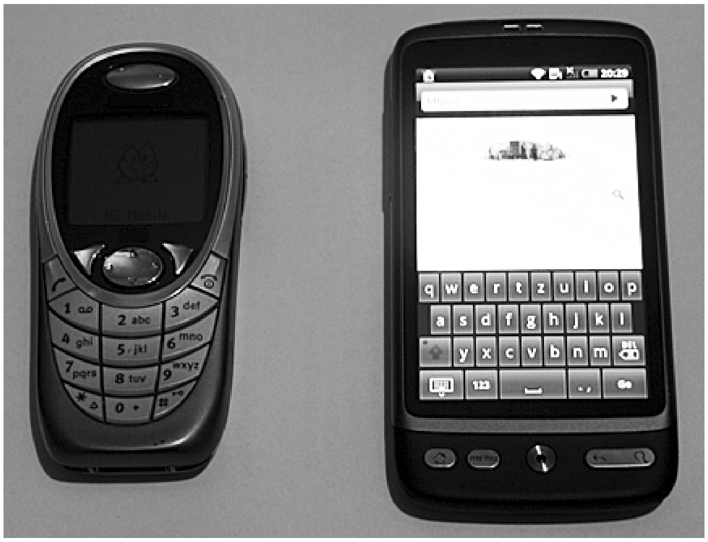

Figure 1.Left: hardware keyboard with a 12-key layout; right: software keyboard with a QWERTZ-layout

Keystroke dynamics with a 12-key layout has already shown its suitability for a biometric authentication on mobile devices. But with the technological changes, they cannot be used in this way anymore. In this paper, we present an approach on the keystroke dynamics for the new capacitive display. For this, we show that the new features can be used to authenticate and distinguish between different users.

In the next steps of this paper, we will briefly describe the related work in Section 2. Then, we will sketch some facts about the keystroke authentication in Section 3 and will focus on the feature extraction in the next section. Section 5 presents the experimental procedure with possible features and classification algorithms. The results of these experiments which are using the classifier are presented in the next section. The last part Section 7 concludes the paper and sketches further work.

2. RELATED WORK

First keystroke dynamic occurred in the desktop computer field in the years between 1985 and 1990 ([6][7]). In this time, studies showed good fault resistance for the keystroke authentication and were improved over the years ([8][9]). Today, keystroke dynamics are already well known in the industry, too.

With the usage of mobile phones 2006 [10], first studies started to adapt the keystroke authentication on the mobile 12-key layout of the phones. Basically, they used the key hold time, which is the time between pressing two keys, and the error rate as features. All these features were extracted via the hardware keyboard.

Buchoux et al. [11] showed two years later that a four-digit long numerical password is too short to authenticate a person. After this, several studies focused on the improvement of error rates ([12][13]). Maiorana et al. [14] used statistical classifier for the keystroke authentication.

With the changes from a 12-key layout of a hardware keyboard to the QWERTZ-layout on virtual keyboards, new challenges occur. For example, there is no physical feedback where the button is pressed. In this paper, we show approaches to get more information of the virtual keyboard than before of the hardware keyboard.

De Luca [15] showed in 2009 how to authenticate with new feature of the capacitive display. He used instead of a keyboard only a 3x3 matrix of points.

3. Biometric authentication

The keystroke dynamic authentication has as all biometric authentications two phases. In the first step, the enrolment, reference features are stored to compare these with the authentication features. The second phase is the actual authentication where a user wants to access something. Both steps are necessary for a biometric authentication.

3.1. Enrolment

The enrolment process has four different steps which are presented in Figure **2**.

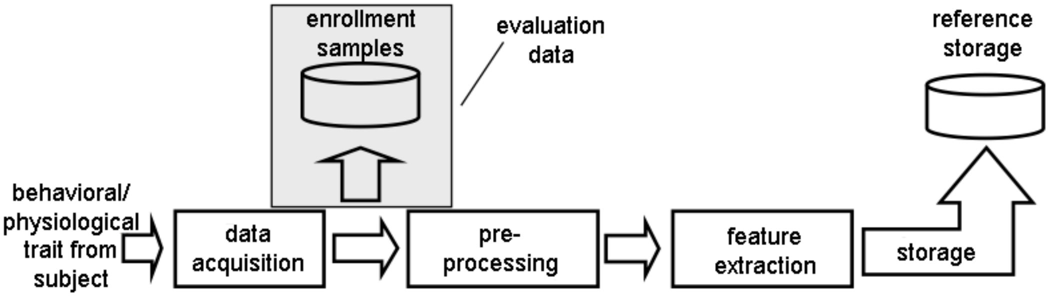

Figure 2. Biometric enrolment process [16]

3.1.1.Data acquisition

Typically keystroke based biometrics generate information from the keyboard (hardware or virtual) at the authentication device. These data are recorded via the operating system and can be stored as a stream of events. After this the raw data are stored as enrolment samples for later evaluations.

3.1.2.Pre-processing

Because biometric features cannot be extracted in the same quality every time, pre-processing has to be done. For example, face recognition depends on the light if it is too dark the picture has to be adjusted (make it brighter).

3.1.3. Feature extraction

The extraction of features is one of the most important steps of the biometric authentication chain. The error rates depend on the selection of the right features. For this, we go more into detail in Section 4.

3.1.4. Storage

The disadvantage of biometric features is that they cannot be done hundred per cent the same way (e. g. movements, speed and pressure). This is a big advantage concerning replay attacks. Authentication attempts are stored in the database. So they can be compared and reply attacks are not working. With the storage of these data, changes can be recognized. For example, handwriting can change over time. This can be recorded to modify the reference data for authentication.

3.2. Authentication

If the data are properly stored for one person in a database (reference storage), the user is able to access the system. For this, he must authenticate himself against the system. The authentication process for this is mainly the same like the enrolment process. Only after the data acquisition, the data are stored as verification samples (to eliminate replay attacks [17]). The last step after the feature extraction is the comparison and classification of the actual data with the data which are stored in the reference storage. This step is used to compare the data from the current authentication process with the storage. Like other biometric modalities, classifiers have been proposed for this comparison including distance measures [6], neural networks ([18][19]) and probabilistic classifier (Bayesian classifier) [20].

Biometric authentication has the disadvantage that some persons are falsely rejected (= false reject rate **-** FRR) and others are false accepted (= false accept rate **-** FAR). This means that on the one hand people who are truly user of the system can be rejected and some intruder can be accepted. A cut in the finger is one problem that a person may not be authenticated. Both error rates should be as low as possible. The problem is that both cannot be zero at the same time and it has to be balanced for the special scenario.

In some literature the EER (= Equal Error Rate) is used instead of FAR and FRR. This is the point where FAR and FRR are equal. But the challenge is to find the right threshold for a situation. Some systems need a low FAR (high threshold) that no intruder can access the system. This is the best solution for high security systems. Other systems have to have a high usability, so it is important that a user does not need to authenticate him five times. In this situation the threshold is smaller compared to the first situation and the FRR is lower. Especially for mobile devices the second approach is more suitable. These different situations are the reason why we used FAR and FRR.

4. FEATURES

The extraction of keyboard features from the device needs first an own application on the mobile device or an own keyboard layout. For the basic features, which are well known for keystroke dynamic, an own application fulfils the tasks, for more advanced features an own keyboard layout is needed.

4.1. Basic features

Typical features for keystroke dynamics are *digraphs*. The digraph characterizes the time between two keyboard events. As we show in Figure **3**, times can be tracked between two different events. One possibility is the time between the events pressing and releasing one key (NpNr **-** N pressing, N releasing), another is between pressing two characters after each other (NpOp). These events have different time stamps. The first case NpNr is the time difference between T3 and T1.

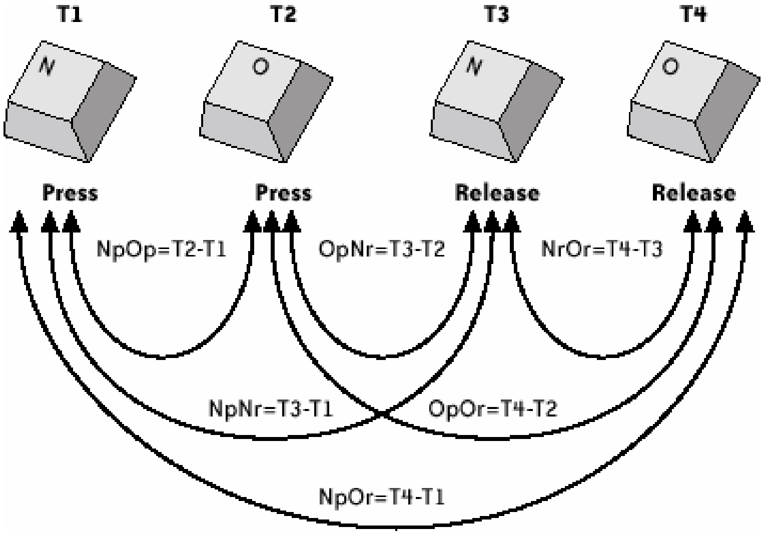

Figure 3. Digraph between letter N and O [21]

Digraphs can be taken from predefined or random words. In the second case because there are no predefined words, the distances between characters on the keyboard are important and whether they are horizontally adjacent. So, adjustments such as horizontal digraph (time to switch between horizontally adjacent keys) or non-adjacent vertical digraph (time to switch between non-vertically adjacent keys) are used [13].

$$s = \sqrt{\Delta x^2 + \Delta y^2}$$

$$t_{norm} = \frac{t_{real}}{s} \; (normalized\ time)$$

The whole distance between the keys can be calculated with the Euclidean distance (function *s*). In combination with the time needed for this a normed value can be generated.

In general, every *n-graph*can be used where the time between a number of n events is tracked. Additionally to the digraph, the most common n-graph is the *trigraph* [22] with three events.
The second most used feature is the*error rate* which indicates the number of times the backspace or delete button is pressed.

Especially on computer keyboards it is important which shift key is used to capitalize letters. Some people are using only one shift key mainly, others are writing using both.

4.2. New features

In addition, some new features can be extracted from the new kind of technology for mobile devices. With the capacitive display of smartphones and tablets, more interactions of the human can be extracted with the device.

The*pressure* during typing can be recorded. This feature is already used in handwriting recognition and can now be adapted for keystroke dynamics.

Furthermore, the *size of the finger* is another feature that is often used. Whether just a part of the fingertip or the whole fingertip is used can be extracted, too. Especially if people are pressing the key only for a short time, normally they are using only a tiny part of their fingertip.

The number of different values for pressure and size of the finger depend on the special mobile device. Normally the amount of different features is for one high (> 100) and for the other smaller (< 20).

With a touch pad, the points where the fingers are pressing can be localized and compared to the *direct position* of the key. So information where the user is pressing the key can be extracted as well. This information could be used instead of the keys which are pressed. Because keys on the touch pad are so small, it happens that the key next to the desired key is pressed. That is why people get stressed and think the usability of the device or application is bad.

Not only has the new capacitive display added features. The device itself can be used to give some more information about the user. The *orientation* of the keyboard shows the preferred carriage. Also the *angle* of the device can be extracted. How a user holds the device is different because the length of his arms is important.

5. EXPERIMENTAL PROCEDURE

Basically keystroke dynamics are used for authentication on a mobile device. Later, it could also be used to re-authenticate during typing emails or phone numbers. For the first evaluation, an application was designed for retrieving basic user information and the authentication information. The application was developed for the Android OS with the Android SDK 14. This application asked the user to type in a specified sequence of letters ten times. If the input is incorrect, he must repeat the sequence. Different smartphones collect a different amount of information that is why we used only one smartphone. The HTC Desire and Samsung Galaxy Nexus are collecting over 100 distinguishing values for pressure but only less than 20 for the size. We used for our experiment a Samsung S2 where the amount of values is the other way around. More than hundred different values for the size and less than 20 for the pressure.

In addition, two new keyboard layouts were developed to investigate and capture all in Subsection 3.1.defined features (e. g. digraph, pressure and fingertip size). The first layout represents the old 12-key layout which was mainly used in mobile phones ten years ago. The second is a full featured QWERTZ-layout. Both are shown in the following Figure **4**.

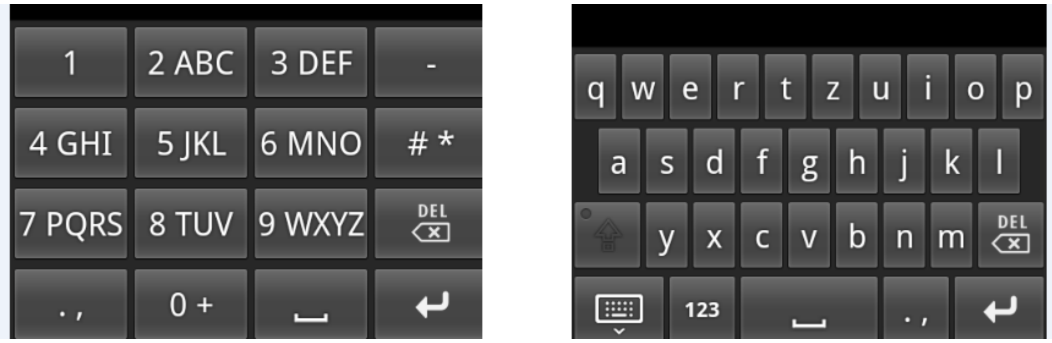

Figure 4.Left: 12-key layout; right: QWERTZ-layout

We focused on two different scenarios. One is the numerical and the other one is the alphabetic input on different keyboard layouts. In each scenario, the smartphone was hold in a vertical way during typing. In the following, the two scenarios are explained in detail.

5.1. Numerical input

To phone with other people it is necessary to type numbers. Two different scenarios were created.

1. Enter 11 times after each other a fixed seven-digit number with the 12-key layout.
2. Enter the same number with a QWERTZ-layout also 11 times.

For both scenarios, it was only possible to write numbers in the field, all other keys were disabled. All 35 participants had to enter the same numbers with each of these key layouts. These participants were all experienced with smartphones and at an age between 25 and 30. Eight instances are used for building reference storage. The remaining three are used to validate the samples (cross validation). Only correct numbers are taken as several previous studies did this for keystroke dynamics ([10][6][20]).

5.2. Alphabetic input

Especially with smartphones, the user is able to write emails or other texts. Also passwords are alphanumeric most the times. In the alphabetic input scenario the user had to enter a 12-digit long alphabetic phrase. The difference between both layouts is that the user has to press the same key twice or more to get all letters. In addition, he has to pause if he wants to get a double letter or another letter on the same key (12-key layout).

The 11 repetitions are also needed as described in Subsection 5.1.and are also separated into information for the reference store and for validation.

6. RESULTS AND DISCUSSION

In this section, we present our results with both keyboard layouts (QWERTY-layout and 12-key layout) and the two input forms (numerical and alphabetic input).

6.1. Numerical input classification

For the classification for each user, a verification sample was created. This was done by taking seven samples of a person and computes the average of this. In addition, the minimum and maximum values for each feature were excluded for fault extraction.

Figure 5 and Figure 6are illustrating the average vectors of five users. The other vectors were also compared to each other, for better visualization only five are printed. All samples are extracted by the input via the QWERTZ-layout.

In Figure 5, the dissimilar digraphs for each key (event) can be seen. These results are from users with some touch pad experiences. For authentication it is important that dissimilarity between all graphs are existing. In this figure, some graphs are straight like the one of the third user which nearly has the same time difference needed for each key. Others show big differences between the single events (like user one). In addition to the straightness, the length for each event can be compared and used to distinguish the users. User one needs in average nearly twice the time the fifth user requires writing a letter.

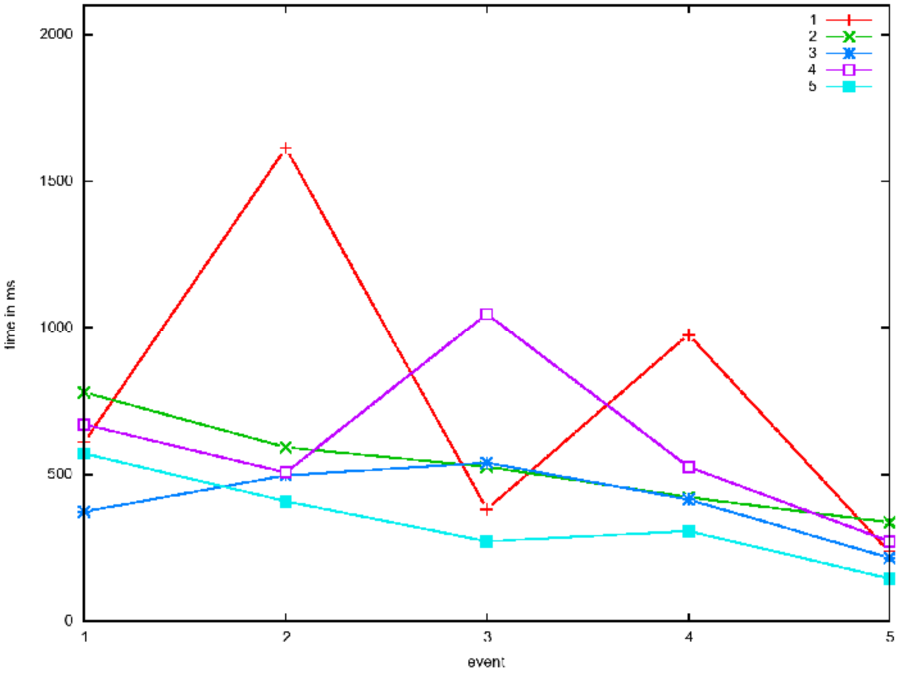

Figure 5.Digraph with QWERTZ-layout (PIN)

Figure 6shows the size of a finger during typing the PIN as well from the same users. The feature finger size shows unique graphs. In comparison to the digraphs, the different size values for the events are more fluctuating for each user.

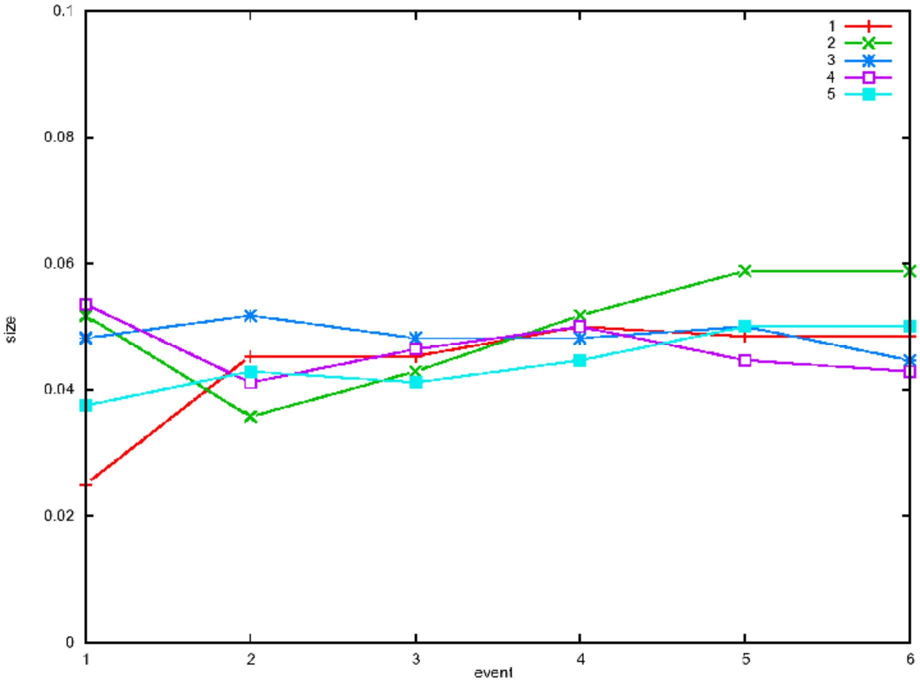

Figure 6.Finger size during pressing different keys with QWERTZ-layout (PIN)

For the input via the 12-key layout, the same differences could be recorded between the users for finger size and digraph. But several differences between these two layouts could be seen as well. The average times needed for the input of the numbers with the 12-key layout was only 89% of the same input with the QWERTZ-layout. In addition, the error rate was 48% lower. Both differences could be explained by the size and order of the keys between both layouts.

On top, the less needed time for the input has influenced the finger size on the key during typing. FAR and FRR between both layouts show also differences like in Table 1shown. FAR and FRR are calculated by the common way [16]:

$$FAR = \frac{\text{number of false acceptances}}{\text{number of impostor identification attempts}}$$

$$FRR = \frac{\text{number of false rejections}}{\text{number of enrollee identification attempts}}$$

Table 1.FAR and FRR for both layouts.

Layout	Average FAR	Average FRR
12-key	9.04%	6.66%
QWERTZ	12.13%	8.75%

The fault rates which are calculated with neuronal networks show the small differences between both layouts but every time there are better results for the 12-key layout.

6.2. Alphabetic input classification

The same approach like seen in Subsection 6.1.was used for the alphabetic input. The dissimilarity could also be seen for the digraph and size of a finger features. These are illustrated inFigure 7 and Figure 8.

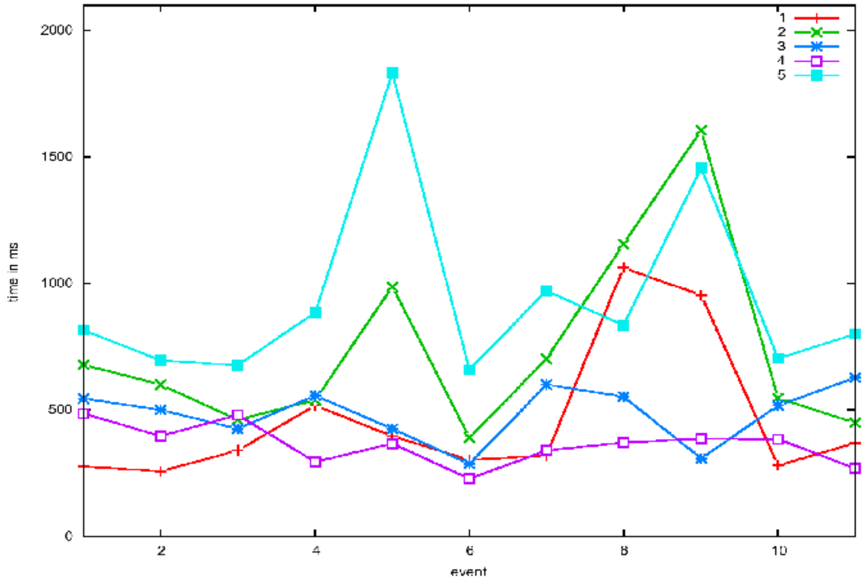

Figure 7.Digraph with QWERTZ-layout (password)

In comparison to the lines of numbers on a QWERTZ-layout (top line), the alphabetic letters are not ordered alphabetically. The layout is the same as on a normal computer keyboard. So some people have to search the letters. This needs time especially for the letters which are not used often. That is why more time in average is needed for typing words and also differs more between single letters.

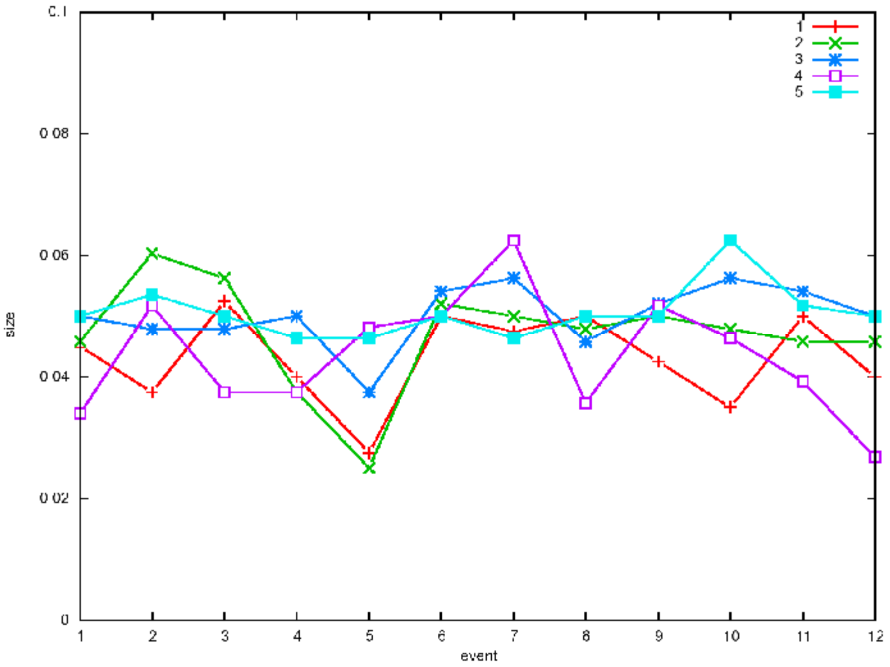

Figure 8.Size of a finger during pressing different keys with QWERTZ-layout (password)

Like with the numerical input we also compared the results of both input forms. Differences could be found as well. The average digraph of the 12-key layout was only 91% of the time needed for the same text with a QWERTZ-layout. But the input of the 12-key layout needed nearly twice the time for the same word (195%). This is easy to explain because for some letters one button must be pressed twice or three times. The error rate was 42% lower with the 12-key layout. The fingertip size during typing was higher as well.

FAR and FRR between both layouts show also differences like in Table 2shown.

Table 2.FAR and FRR for both layouts.

Layout	**Average FAR**	**Average FRR**
12-key	8.31%	5.26%
QWERTZ	9.53%	5.88%

The error rates which are calculated with neuronal networks show the small differences between both layouts as well. In this scenario the results for the 12-key layout showed better results. In comparison to the numerical input, with an alphabetic input both FAR and FRR are better with both keyboard layouts.

7. CONCLUSION AND FUTURE WORK

In this paper, we proposed a new form of keystroke dynamics authentication with a QWERTZ-layout and a capacitive display. The new features are improving the error rates. This means with new hardware devices it is, furthermore, possible to use this biometric method as authentication on mobile devices.

The different keyboard layouts show different error rates which are at a low level. For alphabetic authentication a 12-key layout shows slightly better results than the old QWERTZ-layout. Keys do not need to be pressed multiple times to get one letter for the QWERTZ-layout. If numerical values are only used for authentication, the 12-key layout with bigger keys is better.

Moreover, in combination with the knowledge factor (PIN or password) a strong multi-factor authentication is used which fulfils the requirements of companies as a security level. For this, more experiments must be done to see the resistance of this authentication method. Examples are the text-independent authentication or authentication in different scenarios. But the first results shown in this paper are confident factors that keystroke dynamics can be used for secure authentication using mobile devices. This means either numeric or alphabetic input can be used to authenticate a person. In addition, the statement that the time needed to enter a text depends the size of the keys can be evaluated in more detail. More experiences should be made to show the significance of these features.

With this knowledge it can be researched whether differences exist between authentication with a finger and a pencil. In addition, other input methods can be used for authentication like swyping a word.

REFERENCES

[1] Twentyman, J. (2009) Lost smartphones pose significant corporate risk, http://www.scmagazineuk.com/lost-smartphones-pose-significant-corporate-risk/article/126759/

[2] Imperva(2010) Consumer Password Worst Practices, http://www.imperva.com/docs /WP_Consumer_Password_Worst_Practices.pdf

[3] Nohlberg, M.(2008) Securing Information Assets. Understanding, Measuring and Protecting against Social Engineering Attacks

[4] CNET(2004) Pop-up program reads keystrokes, steals passwords, http://news.cnet.com/Pop-up-program-reads-keystrokes%2C-steals-passwords/2100-7349_3-5251981.html

[5] Apple Inc(2012)iPhone

[6] Umphress, D. & Williams, G.(1985) Identity verification through keyboard characteristics. In: International Journal of Man-Machine Studies, 23, pp. 263–273

[7] Bleha, S.; Slivinsky, C. &Hussien, B.(1990) Computer-Access Security Systems Using Keystroke Dynamics. In: IEEE Trans. Pattern Anal. Mach. Intell, 12, pp. 1217-1222

[8] Monrose, F. & Rubin, A.D.(1997) Authentication via keystroke dynamics. In: Proceedings of the 4th ACM conference on Computer and communications security, pp. 48-56. ACM, New York, NY, USA

[9] Shanmugapriya, D. &Padmavathi, G.(2009) A Survey of Biometric keystrokeDynamics: Approaches, Security and Challenges. In: International Journal of Computer Science and Information Security

[10] Clarke, N.L. &Furnell, S.M. (2006) Authenticating mobile phone users using keystroke analysis. In: Int. J. Inf. Secur, 6, pp. 1-14. Springer-Verlag, Berlin, Heidelberg

[11] Buchoux, A. & Clarke, N.L.(2008) Deployment of Keystroke Analysis on a Smartphone. In: Proceedings of the 6th Australian Information Security & Management Conference

[12] Campisi, P.; Maiorana, E. &Neri, A.(2009) User authentication using keystroke dynamics for cellular phones. In: IET Signal Processing, vol. 3, Issue: 4vol. , pp. 333–341

[13] Zahid, S.; Shahzad, M.; Khayam, S.A. &Farooq, M.(2009) Keystroke-Based User Identification on Smart Phones. In: Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, pp. 224-243. Springer-Verlag, Berlin, Heidelberg

[14] Maiorana, E.; Campisi, P.; González-Carballo, N. &Neri, A.(2011) Keystroke dynamics authentication for mobile phones. In: Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 21-26. ACM, New York, NY, USA

[15] Luca, A. de; Hang, A.; Brudy, F.; Lindner, C. & Hussmann, H.(2012) Touch me once and i know it's you!: implicit authentication based on touch screen patterns.

[16] Vielhauer, C.(2006) Biometric User Authentication for IT Security. From Fundamentals to Handwriting Springer-Verlag

[17] Anjos, A. & Marcel, S.(2011) Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline. In: International Joint Conference on Biometrics 2011

[18] Alsulaiman, F.A.; Cha, J. &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, pp. 114-121. Springer-Verlag, Berlin, Heidelberg

[19] Faundez-zanuy, M.(2005) Study of a Committee of Neural Networks for Biometric Hand-Geometry Recognition. Neural Networks, 1180 - 1187

[20] Monrose, F. & Rubin, A.D.(2000) Keystroke dynamics as a biometric for authentication. In: Future Generation Computer Systems, 16, pp. 351-359. Elsevier Science Publishers B. V.

[21] Cranor, L.F. &Garfinkel, S. (2005) Security and Usability: Designing Secure Systems That People Can Use O'Reilly Media

[22] Choraś, M. &Mroczkowski, P.(2007) Keystroke Dynamics for Biometrics Identification. In: Proceedings of the 8th international conference on Adaptive and Natural Computing Algorithms, Part II, pp. 424-431. Springer-Verlag, Berlin, Heidelberg

Authors

Matthias Trojahn is working for the Volkswagen AG in Wolfsburg, Germany. He did his Master of Science at the Otto-von-Guericke University in Magdeburg. At the moment he is an external PhD student at the Otto-von-Guericke University in Magdeburg with the topic "Multifactor authentication on mobile devices (Smartphones and Tablets)".
Matthias Trojahn is also owner of the CISSP (Certified Information Systems Security Professional) certificate.

Frank Ortmeier is a professor for Computer Systems in Engineering at the Otto-von-Guericke University in Magdeburg. He did his PhD at the University of Augsburg on "Model-based safety analysis" in 2005. His main research interests are in the domain of dependable software-intensive systems. This ranges from analysis of safety critical applications to systems engineering of software intensive applications. In particular, he is researching on interaction of safety and security of cyber-physical systems.

Frank Ortmeier is responsible for a number European exchange programs, member of several international program committees, an active member of the pre-standardization group EWICS, leading a number of academic and industrial research projects on and spokesman of the regional chapter of the German computer society (GI). He is also responsible for the study programs "Ingenieurinformatik" and "Digital Engineering" at the Otto-von-Guericke University.