KeyGait: Framework for Continuously Biometric Authentication during Usage of a Smartphone

Matthias Trojahn
Volkswagen AG
Wolfsburg, Germany
matthias.trojahn@volkswagen.de

Frank Ortmeier
Otto-von-Guericke University
Magdeburg, Germany
frank.ortmeier@ovgu.de

***Abstract*—The ability of having a secure mobile device is determined by different aspects (e.g., hardened system, authentication or anti-virus). Normal authentication methods are only requesting authentication characteristics at the beginning of the usage. The aim of this paper is to create a framework which can continuously analyze which user is using the device at each moment. While mobile devices are easy to lose or can be stolen, it is important to do an authentication process during usage. We propose a continuous trust model using keystroke dynamics and movements of the device as biometrical modalities to have a certainty of the usage at each time.**

***Keywords*—security framework; mobile devices; biometric authentication; continuously authentication; usability**

I. INTRODUCTION

The need of a continuous authentication process exists for mobile devices. These devices can be stolen or lost easily because they are so small. For example, a survey from Credant Technologies reported in 2008 that in six months 55,000 cellular phones were left in London taxis [1]. The first challenge is that these devices are only secured by a password. In addition, only if the device is unlocked properly the password is asked when accessing the device. This means a continuous authentication system with a properly initial authentication combined with a re-authentication during usage is needed. Re-authentication means an additional authentication during usage, which happens in the background.

In this paper, we present a framework which uses inertial sensors and a capacitive display to fulfill the need for the continuous authentication system.

For this, we describe the related work and the contribution of our work in this section. In Section 2, we present our continuous authentication model with the concept and the trust model which handles the certainty of the device which user is using the device. Then, we will present hypothetical test cases for using this model. Finally, we discuss the framework in Section 4 and conclude our research in Section 5.

A. Related work

Two related researchs were identified. First, we will focus on the biometrical authentication via keystroke on smartphones. This can be separated into text dependent or independent analysis. The second approach is concerning the gait recognition of a person.

Prior work for keystroke dynamics was mainly focused on keyboard for a PC [2], [3] or on the mobile phone with 12 keys [4], [5]. Most of the experiments are using the features "duration of pressing one key" or the "time between pressing two / three keys". In general, error rates like *false acceptance rate* (FAR) or *false rejection rate* (FRR) are used to compare different results. The FAR describes how intruders can access a system. In addition, the percentage of rejections of an authorized person divided by all attempts of authorized person is called the FRR. Both error rates have to be as small as possible to have a secure system. The point where FAR is equal to FRR is called *equal error rate* (ERR). Good results for text dependent authentication are already shown by Karatzouni et al. [6] with a EER of 12.2 % (experiment with 50 person). The advantage of keystroke is that not all attempts by an intruder are successful compared with a simple password authentication. A FRR of 12 % means that only every ninth attempt of all unauthorized attempts is successful.

Zahid et al. [7] did a text independent keystroke authentication. They used key hold time, error rate and different digraphs (horizontal, vertical, non-adjacent horizontal and non-adjacent vertical) as features. The different digraphs are used because there is no prediction of the combination between different keystrokes. These experiments on a mobile phone with 12 keys had a result of FAR 11 % and FRR 9.22 %.

As in the survey done by Banerjee [8], a lot of different experiments showed better results then the previous mentioned experiments but there the number of subjects was low (under 50 people).

The gyroscope is employed to measure any rotation of the device. Only the uniqueness for single persons turned out to be rather low. In an experiment Derawi et al. [9] had in the study an EER of 20 % (the device was carried on the hip of the test person). This is not enough to be a good single authentication method. A fusion with the keystroke dynamics is necessary. Further work has shown that with a higher sampling rate the EER can be improved [10], [11]. If more than one smartphone could be used the recognition rate could be reduced [12].

B. Contribution of this work

The major shortcoming of all existing approaches is that they do not allow continuous authentication on smartphones. Keystroke dynamics with a fixed text is only possible during the unlock process. After this, the user is not typing the same pass phrase again. Text independent keystroke authentication is not analyzed properly for the new generation of mobile phones with capacitive display. Gait authentication is an approach which can be used as a continuous authentication but the error rates are too high to give a certainty which is needed for a

 ISBN: 978-1-61208-313-1

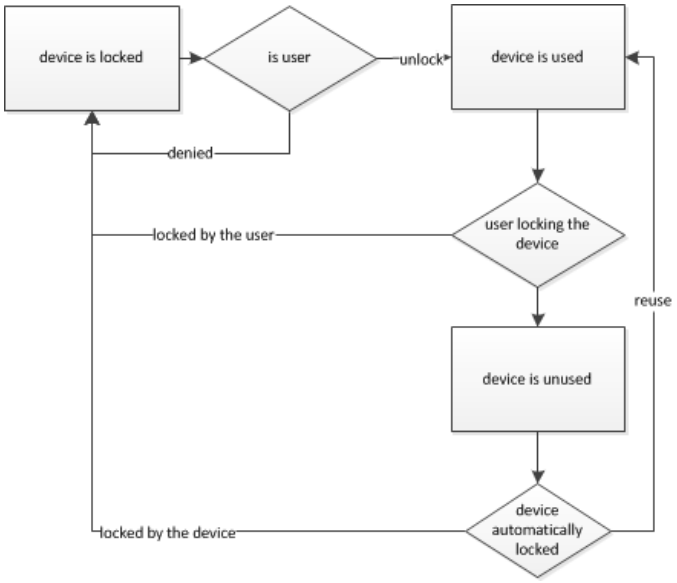

Fig. 1: Activities during usage of a smartphone

secure environment. It only can be used during fusion with another modality.

The goal of this work is to propose a generated framework which can be used to authenticate a person continuously during the whole process of usage. For this, we present a solution using different sensors of smartphones. The solution is based on a trust model where the users are authenticated with a particular certainty.

Fig. 1 describes the whole process of unlocking and locking of a device. If the user wants to use the device, an authentication has to be done. For this task, the keystroke authentication is suitable.

Fig. 1 also shows also which possibilities exist after usage. First, the user locks the device himself. Second, the device is locking itself after a predefined time. The last possibility is that the user wants to use the device again. In this situation it is without a continuous authentication not possible to say whether it is the same user or not. This model which includes a continuous authentication will be described in the next section.

II. Our continuously authentication methodology

The fundament of our model is a fusion of different modalities and a transparent trust measurement. This fusion has to be done continuously while the device is unlocked. First, we will describe which modalities are included, then, we will present the trust model.

A. Concept for a model

There are three basic points where a model can be attached: during the unlocking of the device, during the usage of the device and during the time the device is not used but unlocked.

Only if all points are included in an authentication system it can continuously give information about how certain the temporally user is recognized.

Because we focused on the capacity display and the gyroscope of the device, we could do the initial authentication on

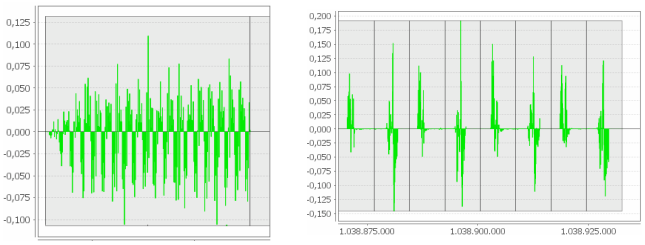

Fig. 2: Data of the gyroscope sensor (Left: Z-axis during walking; Right: X-axis during putting device on table)

the device via keystroke or gait. As we already stated, the error rates for gait recognition are too high to give enough certainty about the user. That is why we propose to use the keystroke in addition to the password which we analyzed previously on smartphones [13]. We suggested in different experiments the usage of the capacitive display to extract additional features (e.g., size of finger during typing or the correct coordinates).

In both of the next use cases, it is demonstrated how the gyroscope data can be used. Fig. 2 shows the changes of the one of three vectors (axis x, y and z - z vector was used). On the left, a person was asked to walk with the device in the pocket for 20 seconds. All the recorded steps show consciously similar changes between different steps. The other two axis show the same similarities which means a function can be created which make it possible to recognize these pattern of values as a walking person. The right figure represents how a device is rotated. At first, the user had to put the device form a table to his pocket and then do it the other way around. In this use case it can be seen how sensitive the data are. Small changes are existing even if the device is placed on a table that means a filter has to be used to extract these incorrect data. After cleaning the data streams different scenarios can be extracted by generating models for use cases (unique combination of the gyroscope values).

In general, it is possible to detect whether the device moves or stays at a location. This is important to trace whether the device was unused by the user. In addition, as already stated, the gait recognition could be used for a re-authentication if the user is walking during using the device.

On the other hand, if the user is typing, the capacitive display can be used to record data and authenticates the user by the behaviour during typing (see Subsection I-A).

Gait and the text independent authentication using keystroke can be used for a re-authentication. This could be used to decide whether the user can reuse the device (see Fig. 1). If no decision could be made or the device is already locked, the user has to authenticate himself via his password.

B. Trust model

In the previous subsection, we described which modalities we use for our framework. Now, we will define a trust model for continuous authentication.

In Fig. 1, all use cases were shown which have to be represented by the model. The device is locked and the user has to authenticate him by using password and his biometric keystroke behavior. Basically, the trust level depends on the initial authentication. A higher certainty ($auth_{intial}$) results in a higher trust level at the beginning of the usage process.

 ISBN: 978-1-61208-313-1

Fig. 3: Scale for the trust model

Furthermore, the time has an important role. With a rising time difference between the initial authentication and the current time the certainty decreases. Only with further re-authentication methods the trust level could rise again. This concept can be represented with the next formulas.

$$trust(t) = auth_{intial} - \alpha \sum_{i=0}^{N} (cert(i)) \tag{1}$$

$$cert(t) = \begin{cases} 0, & if(key(t) \neq null) \ and \\ & (\beta \ move + \chi \ key \geq \delta) \\ \frac{\delta}{2} - \beta \ move(t), & if(key(t) = null) \\ \delta - (\beta \ move(t) & \\ +\chi \ key(t)), & otherwise \end{cases} \tag{2}$$

This means the initial authentication and the decreasing certainty $cert$ during a time box are influencing the trust in which the device know which person is using the device. The time length of the time boxes has to be evaluated in combination with β and χ. During this time box the decreasing certainty is calculated by recognition of the movements of the devices $move(t)$ and the interaction with the capacitive display $key(t)$. Both values are representing the certainty of each sensor whether it is still the same person. They can be between 0 and 100. The value δ describes the threshold which is needed that the trust level does not change. The value $move(t)$ can be walking of the person, text input or a combination. For example, if a user is walking all the time after the unlock it, the trust level should not decrease a lot. The second case represents the case if the user is not using the device (e.g., is in the pocket or is laying somewhere).

Fig. 3 shows the scale for the trust value. The position x represents the initial authentication. The value is influenced by the threshold of the authentication system and the amount in which the authentication value was higher than the threshold. With a bigger difference the $auth_{initial}$ is rising. In Figure 3, additional areas are shown. The trusted area is the range where the device knows who the user is with a specific trust level. If the trust level is under the threshold φ, the device is unsure and the device gets locked (the user cannot be temporally recognized enough). Only with an initial authentication the user could access the device again. Before this could happen, the temporally trust level gets under the value η. Then the certainty is not enough to access all systems. In some companies policies exist where with a one-factor-authentication (password) not every system could be accessed whereas with a two-factor-authentication (public key infrastructure with password) the access is granted. This can be adapted to this model. If the trust is over the trust level η the systems grants access to applications which are normally accessed with a two-factor-authentication. Between point φ and η it could be used as a one-factor-authentication.

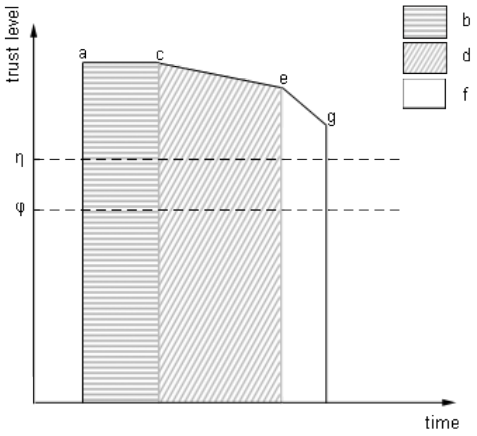

Fig. 4: Trust level for scenario 1

III. HYPOTHETICAL TEST CASES

In this section, we will show how the framework works. For this, we present the steps for two different scenarios. The framework was implemented. For this, the variables (χ, β ...) which are described in the formulas of Subsection II-B have been replaced by the number 1 (naive approach). The time for a time box is set to five seconds.

A. Scenario 1: Trust level is always given

In the first scenario, a user is writing emails while walking (b) after the initial authentication (a). Then, the user stops writing and puts the device in the pocket of his trousers (c). After this, the user is continuing walking (d) and when an email is incoming, he is taking the device out of the pocket (e) and reads the email (f). The last step is the locking by the user (g). All the time the user was over both trust level lines so the trust was high enough for all applications.

Different context changes can be seen in the Fig. 4. The initial authentication has a very high trust value. This has two reasons, first the error rates for keystroke authentication are low (at least under 5%) and second the user was identified with a high certainty. During writing and walking the sensor collects a lot of data. With this it is possible to recognize a person that is why the trust level does not decrease much. Putting the device in and out of the pocket the system recognizes a context change. This can be used in next time boxes. We know with this context changes that the user is still in the position of the device to a very high level. It is, especially, in the situation that the capacitive display is not used because the error rates of gait are higher than the error rates for keystroke.

On the other side, if walking and reading are compared the trust level decreases more because while reading on the device, not enough input is generated to identify a person.

B. Scenario 2: Where an automatic lock happens

The second scenario was generated to show in which situation an automatic lock of a device happens. For this, we

 ISBN: 978-1-61208-313-1

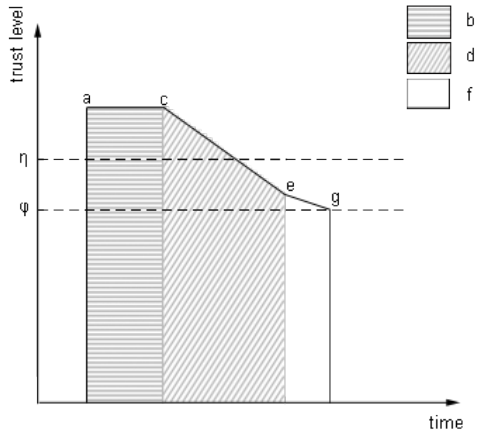

Fig. 5: Trust level for scenario 2

proposed a solution where the device is laying on a table for a non-defined time.

Like the first scenario the start is again an initial authentication (a). After this, the device is unlocked and can be used. Here, the user writes an SMS (b) and after this puts the device on a table (c) and it lays there for a time period (d). Then the user reads a SMS (f) that he just received (e). Then the device is locked (g) because the trust level reached the minimum. In Fig. 5, these steps are shown.

The first two steps are the same like in the previous scenario, one only that a SMS is written. Then, if the user puts the device on a table, both sensors do not get any more data in this case the trust level decreases a lot because the user can be everywhere. During this time the trust decreases under the first trust level line. After this, if the user wants to access a high secure application, a new initial authentication has to be done. While reading the SMS, no input has been done in this case the trust level decreased more until the second line is reached and the device gets locked no matter if the user wants to read the SMS or do other think. In this case the user has to input his initial credentials again to use the device again.

IV. Discussion

This section will discuss this approach and will present some advantages and disadvantages.

With this framework, not only can the trust be established at the beginning of the usage, but even during usage it is possible to recognize the user. For this, no additional interaction has to be done. And no common attack is possible (e.g., shoulder surfing or social engineering) because the additional feature cannot be recorded. That means the security is raised. For comparison, with a password the FAR is 100 %. Together with the knowledge factor this biometric framework could be seen as a two-factor-authentication.

On the other hand, some limitations exist at the moment. The energy consumption for all the required sensors is too high for the general usage during one day. In addition, most of the studies for biometric modalities are not tested in general use cases. All possible movements are not tested how well they can be recognized and the system needs a lot of training to identify the user.

V. Conclusions

In this paper, we first identified the problem of the continuity of an authentication method on smartphones. Therefore, we proposed a continuous authentication method using keystroke dynamics (text dependent and independent) in addition to the movement of the device (e.g., gait recognition). These methods have to be fused and checked during several predefined timed boxes.

We presented a decision model how the trust can be calculated during one and more time boxes. Especially, the introduction of different thresholds is important for using applications with different security level.

We proposed some scenarios, which show how the framework is working, e.g., in which scenario the device locks the device. In addition, advantages and disadvantages are presented.

Overall, the proposed framework is an option for a biometrical authentication on smartphones. It is an important step towards a more effective and continuous authentication.

In the future, more tests have to be done with the modalities, especially, in more general use cases. In addition, the energy consumption has to be reduced.

References

[1] J. Twentyman, “Lost smartphones pose significant corporate risk,” 2009. [Online]. Available: http://www.scmagazineuk.com/lost-smartphones-pose-significant-corporate-risk/article/126759/ [retrieved: 09/2013]

[2] D. Umphress and G. Williams, “Identity verification through keyboard characteristics,” in *Intl. J. of Man-Machine Studies*, 1985, pp. 263–273.

[3] F. Monrose and A. D. Rubin, “Keystroke dynamics as a biometric for authentication,” in *Future Generation Computer Systems*, vol. 16. Elsevier Science Publishers B. V, 2000, pp. 351–359.

[4] S.-s. Hwang, S. Cho, and S. Park, “Keystroke dynamics-based authentication for mobile devices,” in *Computers & Security*, vol. 28, no. 1–2, 2009, pp. 85–93.

[5] A. Buchoux and N. L. Clarke, “Deployment of keystroke analysis on a smartphone,” in *6th Australian Inf. Sec. & Management Conf.*, 2008.

[6] S. Karatzouni and N. L. Clarke, “Keystroke analysis for thumb-based keyboards on mobile devices,” in *Proceedings of the IFIP TC-11 22nd Intl. Inf. Sec. Conf.*, H. S. Venter, M. M. Eloff, L. Labuschagne, J. H. P. Eloff, and R. v. Solms, Eds., 2007, pp. 253–263.

[7] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, “Keystroke-based user identification on smart phones,” in *Intl. Symposium on Recent Advances in Intrusion Detection*, ser. RAID ’09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 224–243.

[8] S. Banerjee and D. Woodard, “Biometric authentication and identification using keystroke dynamics: A survey,” in *Journal of Pattern Recognition Research*, vol. 7, 2012, pp. 116–139.

[9] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive user-authentication on mobile phones using biometric gait recognition,” in *6th Intl. Conf. on Intelligent Inf. Hiding and Multimedia Signal Processing*, Washington, DC, USA, 2010, pp. 306–311.

[10] K. Holien, “Gait recognition under non-standard circumstances,” Ph.D. dissertation, Gjøvik University College - Department of Computer Science and Media Technology, 2008.

[11] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-m. Mäkelä, and H. Ailisto, “Identifying users of portable devices from gait pattern with accelerometers,” in *IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, 2005.

[12] G. Pan, Y. Zhang, and Z. Wu, “Accelerometer-based gait recognition via voting by signature points,” in *Electronics Letters*, vol. 45, no. 22, 2009, pp. 1116–1118.

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

 ISBN: 978-1-61208-313-1