Gesture-based User Authentication for Mobile Devices

Dennis Guse
Quality and Usability Lab,
Deutsche Telekom Laboratories,
Technische Universität Berlin
Ernst-Reuter-Platz 7
10587 Berlin, Germany
Dennis.Guse@telekom.de

Sven Kratz
Medieninformatik,
LMU München,
Amalienstr. 17
80333 München, Germany
Sven.Kratz@ifi.lmu.de

Niklas Kirschnick
Quality and Usability Lab,
Deutsche Telekom Laboratories,
Technische Universität Berlin
Ernst-Reuter-Platz 7
10587 Berlin, Germany
Niklas.Kirschnick@telekom.de

Sebastian Möller
Quality and Usability Lab,
Deutsche Telekom Laboratories,
Technische Universität Berlin
Ernst-Reuter-Platz 7
10587 Berlin, Germany
Sebastian.Moeller@telekom.de

MobileHCI 2011, Aug 30–Sept 2, 2011, Stockholm, Sweden.
ACM 978-1-4503-0541-9/11/08-09.

Abstract
In this paper we present a gesture-based user authentication mechanism for handheld mobile devices. For authentication the user does not enter a password or PIN, but rather moves the device in an individual specific manner. The mobile device measures the movements using a built-in 3D-accelerometer and a 3D-gyroscope. Movement-based biometric features for authentication are considered very useful, because they are memorized differently and especially promising for mobile devices. The implemented mechanism was evaluated in a user study with regard to feasibility, the user perception and security including active attacks.

Keywords
Biometrics, Machine Learning, Perceived Security, Usability, Accelerometer, Gyroscope

ACM Classification Keywords
H.5.2 Information interfaces and presentation: Miscellaneous

General Terms
Algorithms, Security, Experimentation, Human Factors, Measurement

Introduction

Mobile devices are becoming a ubiquitous computing platform. The amount of sensitive personal data stored on mobile devices is steadily rising. Likewise, mobile devices provide access to important services including telephony and mobile internet as well. User authentication is of great importance to guarantee a certain level of security. The most widespread mechanisms are based upon knowledge like PINs and passwords. However, these mechanisms are cumbersome due to the fact that a non-trivial secret needs to be memorized and the input methods on mobile devices are limited.

A lot of mechanisms have been proposed to improve mobile authentication. In this paper a mechanism is presented using hand gestures with which the user moves the device. The device uses a built-in accelerometer and a gyroscope to measure the movement. The user does not memorize an arbitrary secret, but rather trains an individual gestures. This information is stored implicitly in the motoric cortex. For a successful attack it is not sufficient for an attacker to get the knowledge how a gesture is performed, because he also needs to learn mimicking the genuine user's movements while performing the gesture.

The paper is organized as follows: first we give an overview of related work. Second we describe the gesture-based authentication mechanism in detail. Afterwards, we describe the conducted user study and present and discuss the results. Finally, we conclude the work and give an outlook on future work. All details omitted in this paper can be found in Guse [5].

Related Work

Chong et al. [2] extended PIN-based authentication by using ad-hoc gestures mapped to single numbers. The user enters his PIN by moving the device in the corresponding manner. The user is required to learn the specific movements corresponding to the gestures. An approach based upon personalized hand gestures is presented in Okumura et al. [7]. Personalized hand gestures are chosen by the user and should be specific to him. This approach is refined by Matsuo et al. in [6] by adding an update procedure for long term stability. An Equal-Error-Rare (EER) of 5% was achieved in this user study. A similar approach is presented by Guerro Casanova et al. [4]. They achieve an EER of 2.5%. In Farella et al. [3], an approach based upon feature extraction is studied for user identification. They achieved an accuracy of 95%. All presented approaches used only built-in accelerometers to capture the gestures. Also, all approaches except Farella et al. used Dynamic Time Warping (DTW) [9] with a single template to "learn" the genuine gesture.

Gesture-based Authentication Mechanism

In this work a gesture-based authentication for mobile devices with built-in 3D-accelerometer and 3D-gyroscope is presented. We assumed that using an additional but different sensor will improve the performance. For the mechanism the raw measurements of both sensors are used in a threshold-based approach. Using five enrollment samples a model is created and the threshold is calculated. As models variants of DTW and Hidden Markov Models (HMM) were studied. DTW was implemented as presented in Sakoe et al. [9] using the weighted Minkowski Norm. A DTW model consists of one sequence. This sequence is either one of the enrollment samples, i. e. the cheapest

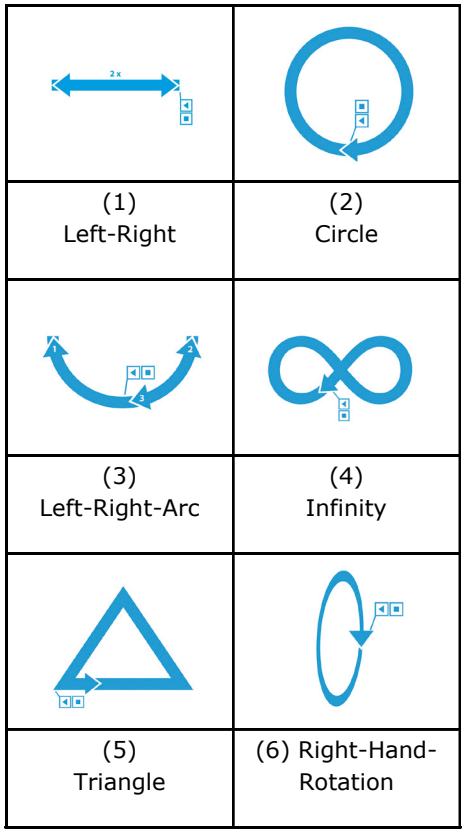

Figure 1: Visualization of the designed gestures used in the genuine part of the conducted user study.

one, or is computed using an adaption of the integrative approach of Abdullah et al. [1]. For DTW the normalized costs of the cheapest path were used as similarity metric. Left-to-Right first-order HMMs with a multivariate Gaussian emission distribution [8] and the normalized likelihood as similarity metric were studied. In addition to the recognition algorithm, a length constraint was applied. It limits the maximal allowed difference in length of unknown samples compared to the enrollment samples mean length.

User Study

The performance of the mechanism was evaluated with a two-stage user study. In the first stage the genuine user perspective was simulated with 15 participants. Each participant individually interpreted the gestures shown in Figure 1. Each participant provided 5 enrollment and 15 validation samples. In the second stage attempts to forge gestures with 10 attackers were studied. For each designed gesture two interpretations of the first stage were attacked using the video recordings of the corresponding enrollment samples.

Three types of forgery were evaluated. Naïve and semi-naïve forgery are accidental forgeries recorded in the first stage. Naïve forgery includes all recorded samples, which are not based upon the same gesture. Semi-naïve forgery includes all samples which are based upon the same gesture, but are not performed by the genuine user. Visual forgery is based upon visual disclosure of the genuine gesture to the attacker using video recordings from different perspectives. The attacker can use the acquired knowledge to create sophisticated forgeries. This is a real threat case for the presented authentication mechanism.

Results

The results of the user study are promising. It was found that a length constraint of 23% performs well. It includes 97.3% of the enrollment and 90.7% of the validation samples, but excludes 58.3% of the naïve and semi-naïve and 36.9% of the visual forgeries without evaluating the trained model.

For HMMs 14-states were found to be optimal. For DTW a slope constraint of 1 and a non-diagonal alignment penalty provided the best results. The integration of multiple samples into a template performed better than choosing the cheapest enrollment sample as model.

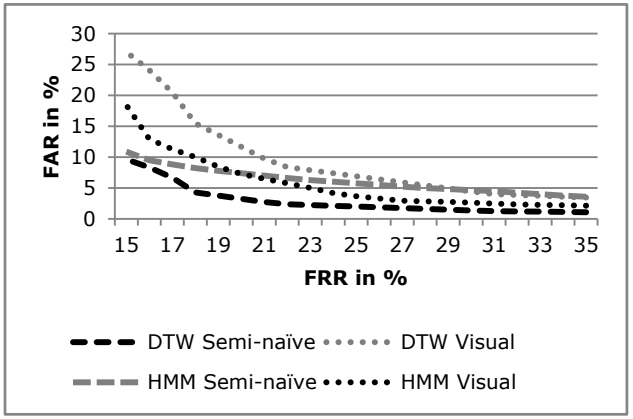

Figure 2: ROC Results for the 12 attacked models in the 2nd stage of the user study.

As expected, naïve forgeries were very seldom accepted as genuine by both algorithms. In Figure 2 the Receiver Operating Characteristics (ROC) of HMM and DTW for semi-naïve and visual forgery are compared for the twelve attacked models. DTW performs as expected, because visual forgeries are

more likely to be accepted as semi-naïve ones. An unexpected result occurred for HMMs. These accept more visually forged samples than semi-naïve ones. This effect seems to be dedicated to the usage of the likelihood as similarity metric. However, HMMs perform by far better for visual forgeries than all studied variants of DTW. In a detailed evaluation of DTW it was found that 5 of the 12 attacked gestures had a False-Rejection-Rate (FRR) less than 20% without accepting any of the visual forgeries. One model achieved 0% FRR and only one model was completely unusable with an FRR of 93%.

None of the participants of the experiment's first stage perceived the mechanism as unnatural, annoying or fatiguing. 10 of them would use gestures for authentication on mobile devices in public places. Nevertheless, 7 participants believed that a gesture is easily forgeable. The majority of forgers believed that they can create an exact forgery for 9 of the attacked gestures. However, as shown with the forgery part of the user study, this is not true. So, non-professional forgers overestimate their skills.

Conclusions and future work

The presented results of the user study prove the feasibility of gesture-based user authentication regarding usability and security using available mobile devices with built-in accelerometer and gyroscope. Overall, gesture-based authentication seems to be a very promising alternative to established authentication mechanism on mobile devices. Future work is required to refine the applied algorithms and study the long term stability of a memorized gesture. Furthermore, social aspects have to be considered and evaluated.

References

[1] Abdulla, Waleed H.; Chow, D.; Sin, G. *Cross-words Reference Template for DTW-based Speech Recognition Systems*, TENCON 2003, 1576-1579.

[2] Chong, M. K.; Marsden, G. *Exploring the Use of Discrete Gestures for Authentication*. Proc. INTERACT 2009, Springer, 205-213.

[3] Farella, E.; O'Modhrain, S.; Benini, L.; Riccó, B. *Gesture Signature for Ambient Intelligence: A Feasibility Study*. LNCS Vol. 3968, Springer, 2006, 288-304.

[4] Guerra Casanova, J.; Sánchez Ávila, C.; de Santos Sierra, A.; Bailador del Pozo, G.; Jara Vera, V. *A Real-Time In-Air Signature Biometric Technique Using a Mobile Device Embedding an Accelerometer.* CCIS Vol. 87, Springer, 2010.

[5] Guse, D. *Gesture-based User Authentication for Mobile Devices (Master Thesis)*, TU Berlin, 2011.

[6] Matsuo, K.; Okumura, F.; Hashimoto, M.; Sakazawa, S.; Hatori, Y. *Arm Swing Identification Method with Template Update for Long Term Stability*. LNCS Vol. 4642, Springer, 2007, 211-221.

[7] Okumura, F.; Kubota, A.; Hatori, Y.; Matsuo, K.; Hashimoto, M.; Koike, A. *A Study on Biometric Authentication based on Arm Sweep Action with Acceleration*. Proc. ISPACS 2006, IEEE, 219-222.

[8] Rabiner, L. R.; Juang, B. H. *An Introduction to Hidden Markov Models*, ASSP Magazine, Vol. 3, IEEE, 1986, 4-16.

[9] Sakoe, H.; Chiba, S. *Dynamic Programming Algorithm Optimization for Spoken Word Recognition*. IEEE Transactions on Acoustics, Speech and Signal Processing, Vol. 26, 1978, 43-49.