Gesture-based User Authentication for Mobile Devices using Accelerometer and Gyroscope

Dennis Guse, Benjamin Müller

Quality and Usability Lab, Telekom Innovation Laboratories,
Technische Universität Berlin
{dennis.guse, benjamin.mueller}@campus.tu-berlin.de

Art der Arbeit: Master-Thesis in Informatik
Betreuer/in der Arbeit: Prof. Dr.-Ing. Sebastian Möller und Prof. Dr. Michael Rohs

Abstract: In this paper a user authentication mechanism for handheld mobile devices using hand gestures is presented. To authenticate a prior chosen hand gesture needs to be repeated. The mobile device uses a 3D-accelerometer and a 3D-gyroscope to measure the resulting device movement. With a user study it was shown, that the presented approach is feasible and has advantages with regard to usability over widespread knowledge-based authentication mechanisms like PINs and passwords on mobile devices. In a second study a realistic attack vector using video recordings was simulated. The results show that repeating an observed gesture similar enough is a very challenging task.

1 Introduction

Mobile devices offer lots of possibilities and a feeling of freedom to their users as they can be used almost everywhere and at any time. However, this freedom comes along with new security threats as mobile devices store a lot of sensitive information and provide access to important services [BE01]. In fact, unauthorized persons can gain access to mobile devices as for example they can get lost or stolen. To provide security, it needs to be verified that the current user is authorized to use the device. For mobile devices user authentication mechanisms based upon knowledge are widespread like PINs and passwords. Those are easy to implement and well understood by users. However, knowledge-based mechanisms require memorizing a non-guessable secret over a long period of time and everyone knowing this secret can successfully authenticate. On mobile devices those mechanisms are further restricted due to limited text input capabilities. In fact, implementing authentication mechanisms does not necessarily enhance security as genuine users may not use or circumvent unusable mechanisms [Re05]. To be successful an authentication mechanism needs to be fast, reliable and comfortable to use for the genuine users [AS99].

In this paper a user authentication mechanism based upon personalized hand gestures for handheld mobile devices is presented, which is introduced in the following section. Section 3 discusses the implementation and the approach to evaluate the mechanism. This paper closes with the results of the evaluation and gives an outlook on future work.

2 Gesture-based User Authentication

Gestures are expressive body movements and naturally used in human communication. User interfaces using gestures are promising as they allow creating intuitive and natural interfaces for human computer interaction. In prior work it was shown that user movements are an alternative for pairing multiple electronic handheld devices [PPA04, MG09]. For authentication on mobile devices interface designed hand gestures have been found useful [CM09]. However, such mechanisms should only be used in a secure environment as the gestures are potentially easy to observe and to mimic. Farella et al. presented a gesture-based identification mechanism for mobile devices using personalized gestures [Fe06]. A personalized authentication mechanism was also presented by Okumura et al. [Ok06] and refined by Matsuo et al. [Ma07].

The presented gesture-based mechanism is designed for mobile devices, which are mainly used one-handed. In the enrollment process the genuine user choses freely a hand gesture, which he likes to use for authentication. A valid gesture is made holding the device in one hand. It needs to be repeatable. In the authentication process the current user is requested to repeat the prior chosen gesture and authentication succeeds, if the gesture could be reproduced. The usage of gestures for authentication on mobile devices has some advantages over knowledge-based mechanisms. The way how to move is memorized by humans implicitly during training in the motoric cortex, which is not prone to information overload and forgetting [KFR10]. In addition, a gesture cannot be written down or disclosed to other persons easily as it is a movement over time. Also, the available input space is vastly larger and authentication can be done eyes-free. However, humans cannot repeat a gesture completely similarly and the authentication mechanism must allow some variances including path, rotation as well as timing.

3 Implementation and Evaluation

The presented gesture-based authentication mechanism [Gu11] is implemented using a 3D-accelerometer and 3D-gyroscope. These sensors measure the motion indirectly, so the absolute path and orientation cannot be derived, but require little energy and are already built-in in modern mobile devices. To avoid computation and make the mechanism more robust a manual segmentation approach using a push-to-gesture button is used. Continuous First-order Hidden Markov Models (HMM) [Ra89] and Dynamic Time Warping (DTW) [SC78], two machine learning techniques, are used in the authentication process to decide, if the recorded measurements of a movement are similar to the chosen genuine gesture. In addition, the *Length Constraint* is introduced to limit the global variances in timing. To train the machine learning model and calculate the Length Constraint the genuine user provides samples of his genuine gesture.

The presented gesture-based authentication mechanism was evaluated in two user studies using an iPhone 4. In the first study feasibility and usability with 15 participants, which simulated genuine users, were explored. Each subject provided 25 samples of his individual interpretation of six pre-defined gestures, which were presented as a 2D image of the general path and a short description.

The goal of the second study was to prove resistance against skilled attacks [BLM07]. 10 participants acted as forgers using video recordings of the first user study. Three types of attack were studied: *Naïve Forgery*, *Semi-naïve Forgery*, and *Visual Forgery*[1]. Naïve Forgeries are samples created in the first user study based upon another pre-defined gesture. Semi-naïve Forgeries are based upon the same pre-defined gesture, but not the same subject. Visual Forgeries were created by the forgers using the video recordings only. The quality of the forgeries should increase from Naïve to Visual Forgeries as more details about the used interpretation of the gesture are available. The collected data was evaluated offline using 5 samples for enrollment and the rest as forgeries.

4 Results and Future Work

The results of the user studies showed that gesture-based authentication is perceived as a usable alternative to PINs and passwords on mobile devices. The genuine participants found the mechanism not exhausting or annoying. On the one hand, two thirds of them would use such a mechanism in public places. On the other hand, the forger participants assumed that they can learn the gestures quite easily and reproduce them precisely. In contrast to this assumption, the collected data of both user studies shows that the implementation of the gesture-based authentication mechanism is feasible and robust against attacks. Figure 1 shows the Receiver Operating Characteristic (ROC), that is the tradeoff between the False-Acceptance-Rate and the False-Rejection-Rate, for Semi-naïve and Visual Forgeries depending on the allowed variance. The data shows that DTW performs better for Naïve and Semi-naïve Forgery, but HMM outperforms DTW for Visual Forgeries, i.e. realistic attacks.

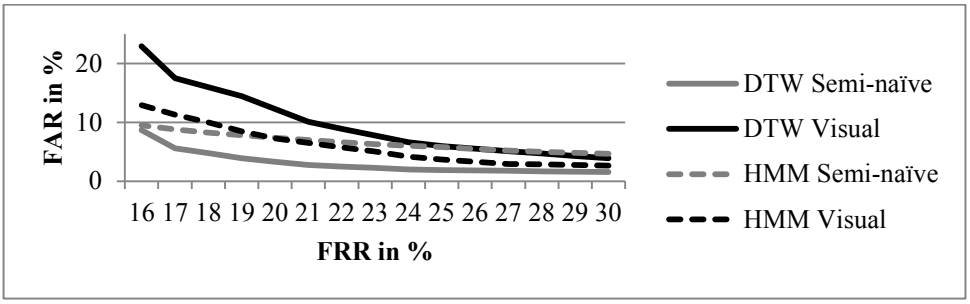

Figure 1: ROC diagram of DTW and HMM for Semi-naïve and Visual Forgery.

The results of the user studies show that the gestures-based authentication is feasibly as well as usable on mobile devices with built-in 3D-accelerometer and 3D-gyroscope. Overall, gesture-based authentication is a very promising alternative to established authentication mechanisms although the performance is lower than for standard PIN authentication. Future work is required to refine the applied algorithms and study the long term stability of memorized gestures. Also, social aspects have to be considered and evaluated. Gesture-based authentication may be a promising alternative to widespread knowledge-based authentication mechanisms.

[1] Based upon the classification of [BLM07].

References

[AS99] Adams, A.; Sasse, M. A.: Users are not the Enemy. Communications of the ACM. December 1999, Vol. 12, No. 42, pp. 41-46.

[BLM07] Ballard, L.; Lopresti, D.; Monrose, F. Forgery Quality and is Implications for Behavioral Biometric Security. IEEE Transactions on Systems, Man, and Cybernetics. October 2007, Vol. 37, No. 4, pp. 1107-1118.

[BE01] Baumgarten, U.; Eckert, C.: Mobile, but Nevertheless secure? it+ti - Informationstechnik und Technische Informatik. 2001, Vol. 43, No. 5, pp. 254-263.

[CM09] Chong, M. K.; Marsden, G.: Exploring the Use of Discrete Gestures for Authentication. Tom Gross et al. (Eds.). Lecture Notes in Computer Science: Human-Computer Interaction – INTERACT '09. Heidelberg, Germany : Springer, 2009, Vol. 5727, pp. 205-213.

[Fe06] Farella, E., et al.: Gesture Signature for Ambient Intelligence: A Feasibility Study. Kenneth Fishkin, et al. (Eds.). Lecture Notes in Computer Science: Pervasive Computing. Heidelberg, Germany : Springer, 2006, Vol. 3968, pp. 288-304.

[Gu11] Guse, D.: Gesture-based User Authentication on Mobile Devices using Accelerometer and Gyroscope, Master-Thesis, Technische Universität Berlin, May, 2011.

[KHT06] Klemmer, S. R.; Hartmann, B.; Takayama, L.: How Bodies Matter: Five Themes for Interaction Design. DIS '06 Proc. of the 6th Conf. on Designing Interactive Systems. June 26-28, 2006.

[Ma07] Matsuo, K., et al.: Arm Swing Identification Method with Template Update for Long Term Stability. Seong-Whan Lee and Stan Li. (Eds.). Lecture Notes in Computer Science: Advances in Biometrics. Heidelberg, Germany : Springer, 2007, Vol. 4642, pp. 211-221.

[Ok06] Okumura, F. et al.: A Study on Biometric Authentication based on Arm Sweep Action with Acceleration. ISPACS '06. Int. Symposium on Intelligent Signal Processing and Communications. December 12-15, 2006, pp. 219-222.

[MG09] Mayrhofer, R.; Gellersen, H.: Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. IEEE Transactions on Mobile Computing. 8, 2009, Vol. 8, 6, pp. 792-806.

[PPA04] Patel, S. N.; Pierce, J. S. and Abowd, G. D.: A Gesture-based Authentication Scheme for Untrusted Public Terminals. UIST '04 Proc. of the 17th annual ACM Symposium on User Interface Software and Technology. October 24-27, 2004.

[Ra89] Rabiner, L. R.: A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. Proc. of the IEEE. 1989, Vol. 77, 2, pp. 257-286.

[Re05] Renaud, K.: Evaluating User Authentication Mechanisms. Lorrie, Faith Cranor and Simson Garfinkel (Eds.). Security and Usability. Designing Secure Systems that People Can Use Editors, O'Reilly, 2005, pp. 103-128.

[SC78] Sakoe, H. and Chiba, S.: Dynamic Programming Algorithm Optimization for Spoken Word Recognition. IEEE Transactions on Acoustics, Speech and Signal Processing. 1978, Vol. 26, No. 1, pp. 43-49.