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

Dennis Guse and Benjamin Müller

Idea: Unlocking your mobile device using your individual 3D-gesture

The current user authenticates by performing his gesture with the device holding hand.
A 3D-gesture consists of the path, device orientation and the timing.

Advantages:

- *Performing*
  Performing a 3D-gesture should be easy, fast and satisfying.
- *Memorization*
  The way how to perform a movement is stored in the motoric cortex, which is not prone to information overload and forgetting. [KHT06]
- *Eyes-free*
  The user can authenticate without looking at the mobile device.

Figure 1: Exemplary posture of one handed interaction with a mobile device.

Requirements

To be a successful alternative, the authentication mechanism needs to be *technically feasible* and achieve [AS99]:

- *Usability*
  The mechanism needs to be usable and suiting to the interaction style of the device and the user.
- *Security*
  The mechanism needs to resist skilled attacks and prevent the genuine user from circumventing the mechanism.

Implementation: Using embedded motion sensors

We implemented the mechanism prototypically using an iPhone 4 using:

- *3D-accelerometer*
  The accelerometer measures the absolute acceleration along all three axes.
- *3D-gyroscope*
  The gyroscope measures the rotational speed around all three axes.
- *Push-to-gesture-button*
  We used a manual segmentation technique. On starting his gesture, the user needs to press the button, hold it and release it on finishing his gesture.

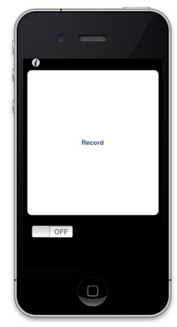


Figure 2: User interface of the implemented Gesture Recorder Application.

The sensor readings of one sample are shown below:

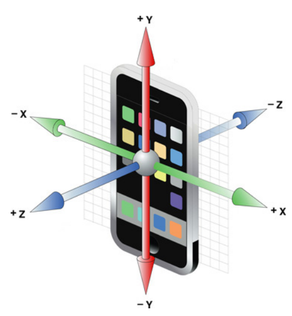


Figure 3: Sensor axes of an iPhone 4 (Source: Apple).

Algorithms

We used machine learning techniques to compute the similarity of an unknown sample and the genuine samples provided by the genuine user in the enrollment process. These can be applied directly to sequential data:

- *Dynamic Time Warping (DTW)* [SC78]
  We applied 38 different variants of DTW. As similarity metric we used the normalized costs of the cheapest path. For training we used either the best fitting enrollment sample or an integrative approach adapted from [AWS03].
- *Hidden Markov Models (HMM)* [Ra89]
  We applied First-order HMM using a multivariate Gaussian emission distribution. As similarity metric we used the normalized log-likelihood.

Length Constraint

In addition we developed the *Length Constraint*, which limits the differences in overall timing of an unknown sample and the mean of the enrollment samples and can be evaluated in *O(1)*.

For *successful authentication,* an unknown sample needs to fulfill the Length Constraint. If this holds, the trained machine learning model is evaluated using a threshold-based approach.

Evaluation Procedure

- *User Study I: Feasibility and Usability*
  We recruited 15 right-handed participants and prepared 6 gestures (see one example in Figure 5.) which the participants interpreted on their own incl. size, timing etc.
  Each participant provided 25 samples per interpretation.
- *User Study II: Breakability*
  In the first study we recorded the participants from three perspectives (see Figure 4).
  We selected 12 interpretations and showed the video recordings to 10 new participants acting as forgers.
  Each participant provided 10 samples per attacked interpretation.

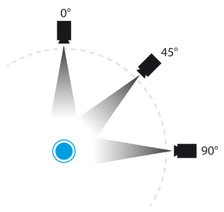


Figure 4: Camera setup.

The genuine users perspective: Feasibility and Usability

The genuine participants of *User Study I* found the mechanism usable:

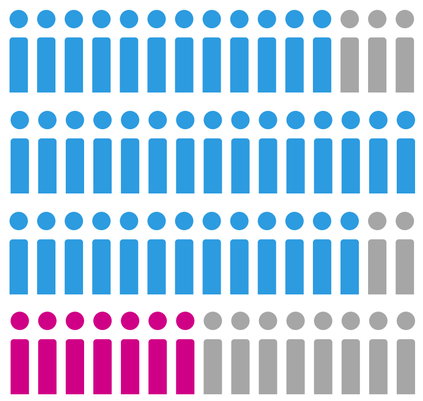


Figure 5: Visualization of the *Infinity* gesture.

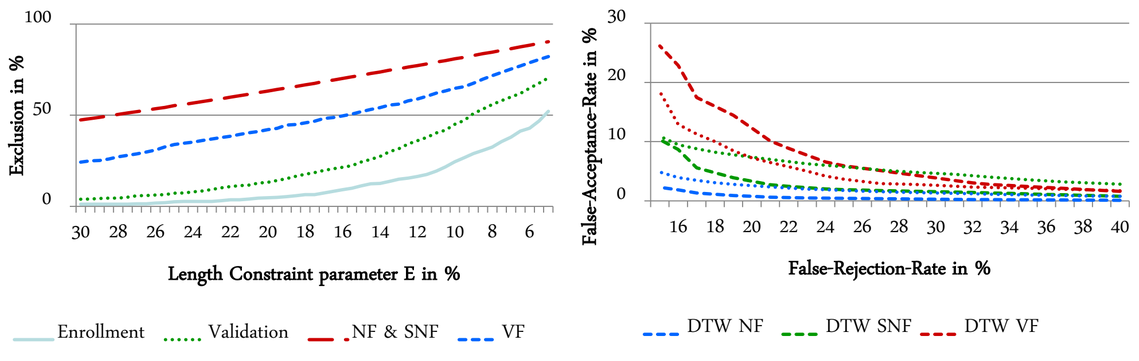
Textual description:
Move the device starting in direction of the arrow in parallel to your upper torso. Start and finish the gesture at the position of the play- and stop-symbol.

The attackers perspective: Breakability

We studied 3 types of forgeries (based on [BLM07]):

- *Naïve Forgery (NF)*
  The attacker has no knowledge about the genuine gesture and can only try brute-force.
- *Semi-naïve Forgery (SNF)*
  The attacker knows the general shape, i.e. the visualization, but has not seen the genuine gesture.
- *Visual Forgery (VF)*
  The attacker was able to observe the genuine user in the authentication process.

The results of *User Study II* with regard to the forgery types are shown below:



Conclusion

The presented user authentication mechanism was found feasible and shows potential to be an alternative to established authentication mechanisms on mobile devices.

Future work is required on:

- Long-term usability and acceptance studies,
- Alternative attacks,
- Additional and alternative sensors.

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.

[AWS03] Abdulla, W. H., Chow; D. and Sin, G.: Cross-words Reference Template for DTW-based Speech Recognition Systems. TENCON 2003. October 15-17, 2003, Vol. 4, pp. 1576-1579.

[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.

[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.

[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.

[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.

Acknowledgments

We like to thank Prof. Dr.-Ing. Sebastian Möller, Prof. Dr. Michael Rohs, Niklas Kirschnick and Sven Kratz for their time, ideas, advices on their on going support.

For further information

Please contact Dennis Guse (dennis.guse@telekom.de).