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.
- Eye-free
  - The user can authenticate without looking at the mobile device.

Requirements

To be a successful alternative, the authentication mechanisms need to be technically feasible and achieve (AF99):
- Usability
  - The mechanism needs to be usable and matching 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.

The sensor readings of one sample are shown below:

![Sensor readings of one sample](image)

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 phase. These can be applied directly to sequential data:
- Dynamic Time Warping (DTW) [SC78]
- Hidden Markov Models (HMM) [Ra89]

By the genuine user in the enrollment process. These can be applied directly to sequential data:

![Algorithms](image)

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

The attacker has no knowledge about the genuine gesture and can only try brute-force.

The attackers perspective: Breakability

We studied 3 types of forgeries based on [BLM07]:
- Naive Forgery (NF)
- Semi-naive Forgery (SNF)
- Visual Forgery (VF)

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

<table>
<thead>
<tr>
<th>Forgery Type</th>
<th>Length Constraint passed</th>
<th>DTW NF</th>
<th>DTW SNF</th>
<th>DTW VF</th>
<th>HMM NF</th>
<th>HMM SNF</th>
<th>HMM VF</th>
</tr>
</thead>
<tbody>
<tr>
<td>NF</td>
<td>0.75</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNF</td>
<td>0.75</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VF</td>
<td>0.75</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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


Acknowledgments

We like to thank Prof. Dr.-Ing. Sebastian Müller, Prof. Dr. Michael Rohr, Niklas Kirschschø and Sean Kreis for their time, ideas, advice on our going support.

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