Biometric Authentication Through a Virtual Keyboard for Smartphones and Tablets

Matthias Trojahn
Student Conference on Software Engineering and Database Systems
July 6, 2012
Motivation - Problems

- something you know
  - insecure passwords (too short, too simple)
  - social engineering
  - key logger

- something you have
  - easy to lose
  - can be stolen

→ something you are
Biometric Authentication

Features

- common features
  - digraph (in general: n-graph)
  - error rate

- new features
  - pressure during typing
  - size of the finger
  - exact localization
  - orientation
  - angle
Experimental procedure

- app for Samsung S2 device (Android SDK 4.0)
- two keyboard layouts
  - 12-key layout
  - QWERTZ-layout
- two scenarios
  - numerical input
  - alphabetic input
Results – numerical input classification (PIN)

- only QWERTY-layout

<table>
<thead>
<tr>
<th>layout</th>
<th>average FAR</th>
<th>average FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-key</td>
<td>4.05</td>
<td>3.38</td>
</tr>
<tr>
<td>qwertz</td>
<td>5.41</td>
<td>4.73</td>
</tr>
</tbody>
</table>
Results – alphabetic input classification (password)

- only QWERTY-layout

<table>
<thead>
<tr>
<th>layout</th>
<th>average FAR</th>
<th>average FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-key</td>
<td>3.38</td>
<td>3.2</td>
</tr>
<tr>
<td>qwertz</td>
<td>2.7</td>
<td>2.03</td>
</tr>
</tbody>
</table>
Conclusion and future work

- new form of keystroke dynamics authentication
- two different layouts
- showed good error rates
- keystroke authentication on touchpads is possible
- different scenarios have to be tested
- other input methods: swype
Thanks.