Exploring Intentional Behaviour Modifications for Password Typing on Mobile Touchscreen Devices

Lukas Mecke\textsuperscript{1,2\dag}, Daniel Buschek\textsuperscript{2\dag}, Mathias Kiermeier\textsuperscript{2\dag}, Sarah Prange\textsuperscript{1,3,2\dag}, Florian Alt\textsuperscript{3}

\textsuperscript{1}University of Applied Sciences Munich, Munich, Germany, \{firstname.lastname\}@hm.edu

\textsuperscript{2}LMU Munich, Munich, Germany, \dag \{firstname.lastname\}@ifi.lmu.de, \dot{\dag}mathias.kiermeier@gmail.com

\textsuperscript{3}Bundeswehr University Munich, Munich, Germany,\{firstname.lastname\}@unibw.de
Motivation

- Premise for behavioural biometrics: behaviour is hard to intentionally change and imitate
- But: Successful mimicry attacks on behavioural biometric systems using technical support [1]

Motivation

• Potential assuming behaviour is controllable:
  – Extending password space for additional security
  – Actively protecting biometric traits by modifying them
  – Recover from leakage (problem with immutable traits)
Are people capable to intentionally modify their (keystroke) behaviour?
Roadmap

• Choose suitable **keystroke features**
• Find **visualisation** to communicate feature modifications
• Study design to foster **exploration** of
  – Participants *ability* to modify their behaviour
  – *Factors* influencing this ability
Keystroke Feature Selection

- 24 Features proposed by Buscheck et al. [1]
- Correlation analysis by Khan et al. [2] → 6 features
- Reduction to 4 features:
  - (touch) area (← pressure)
  - flight time
  - hold time
  - (touch-to-key) offset (← x,y)

---

Pre-study

• **Goal:** Communicate behaviour modifications
• Exploration of *mark-up* and *pictorial* designs
• **Online study** (N=114) with two designs:
  Task: *Associate visualisation with given features*
• **Results** for winning design:
  – Correct attribution rate > 80% for all features
  – Rated *intuitive* and *readable* (agree)
  – Preferred by 59% of the participants
Proposed text annotations

touch area

hold time

touch-to-key offset

flight time
Study design

- Within subject lab study
- 24 participants (14 female, mean age 27)
- 37 Tasks to explore:
  - Different passwords\textit{(password, football, princess)}
  - Different feature\textit{modifications (offset, flight time, hold time, area)}
  - Different\textit{locations (start, middle, end)}
  - Different feature\textit{combinations (0-4)}
  - Different\textit{distribution (distributed or co-located)}
Study design

Unmodified behaviour

Repeated measures design with number x distributed x session

All features in isolation
Procedure

• Two sessions with each
  – Execute tasks (counterbalanced) on our test device with the right thumb (training with feedback, task without)
  – Experience sampling after each task
  – Create or reproduce a custom password

• Concluding Interview
Results

- Natural behaviour
  - Offset towards *bottom right* [1]
  - Secondary peak in flight time for *double letters*
  - Correlation of touch area and key x-position (*thumb stretching*)

Results

• Modified behaviour
  – Successful modification for all features
  – Secondary peaks indicating user errors
Results

• Errors by *target* and *session*
  – Error for offset right significantly smaller than the others
  – Significant session effect for flight time
  – Generally default error was significantly smaller than modified
Results

- Errors by *number* and *distribution* of modifications
  - *Offset remained stable*
  - *Co-located* features resulted in significantly lower error
  - Increased *number* of modifications significantly increased error
Results

• Meta data and subjective ratings
  – Increased *task completion time* for more modifications and for distributed modifications
  – Decreased *typing speed* for more modifications and for distributed modifications
  – More *incorrect password entries* for distributed modifications
  – Co-located modifications were perceived subjectively easier
    (Likert ratings: better able to adjust, higher success, less difficult)
Results

• *Impact on individuality* (Gaussian mixture model for user identification)
  – *Biometric value is decreased* by following modifying towards the same target
  – Some individuality remains
User Feedback

• Hard to control:
  – Offset modifications (hitting the wrong key)
  – Distinguish large area and long hold time

• Creation Strategies:
  – Emphasis

"When I created the password I first typed it and observed what I automatically did. For example I typed a ‘g’ rather to the left, entered a ‘b’ rather [long]; That’s what I adjusted [the password] to."

  – Salient positions (password)
Extending password space

• Detecting Modifications technically feasible:
  – Random Forest Classification (100 trees) with default parameters
  – Leave-one-out validation across sessions
  – Results: accuracy > 94% for all features

• (Upper bound) entropy, assuming random passwords with random modifications (|Σ|=72)

<table>
<thead>
<tr>
<th>password length</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>no modifications</td>
<td>49.36</td>
<td>43.19</td>
<td>37.02</td>
<td>30.85</td>
</tr>
<tr>
<td>1 modification</td>
<td>55.14</td>
<td>48.77</td>
<td>42.38</td>
<td>35.94</td>
</tr>
<tr>
<td>2 modifications</td>
<td>59.84</td>
<td>53.27</td>
<td>46.63</td>
<td>39.90</td>
</tr>
<tr>
<td>3 modifications</td>
<td>63.90</td>
<td>57.10</td>
<td>50.20</td>
<td>43.16</td>
</tr>
</tbody>
</table>
Extending password space

• But:
  – Effect of different keyboard layouts and hand postures
  – Potential common patterns reducing entropy
  – Practically: Requires capturing hardware on all devices

→ Questions for future work
Take away

- Participants are able to intentionally control typing behaviour
- Using modifications to extend password space is possible
- Modifying less and co-located features is easier
- New perspective on typing behaviour (implicit $\rightarrow$ explicit)

Contact: Lukas Mecke
lukas.mecke@ifi.lmu.de