On the Usability and Security of Pseudo-signatures

Jin Chen, Daniel Lopresti,

Computer Science & Engineering
Lehigh University
{jic207, lopresti}@cse.lehigh.edu
Motivation

- How many textual passwords have you been using? Just a few?
- How often do you forget them? Almost always?
- Any passwords from any birthdates, phone numbers, pet’s names?

Using a “pen” to solve this:
signatures, passphrases, graphical passwords, etc.
Motivation

• People usually have only one signature.

• Handwritten passphrases are vulnerable to generative attacks using population statistics\cite{1}.

• “Draw-a-Secret”\cite{2} overcomes some of these flaws, but has its own issue, such as predictable symmetry, centering, etc\cite{3}.


On the Usability and Security of Pseudo-signatures
Jin Chen, Daniel Lopresti,
On the Usability and Security of Pseudo-signatures

Jin Chen, Daniel Lopresti,

Pseudo-signatures

Suggested interpretations on visual cues

• **Color**: writing speeds
• **Number**: stroke orders
• **Arrow**: stroke directions
• **Dashed Line**: stroke format
• **Gray Circle**: dwellings

**Note all the instructions on cue interpretations are vaguely described to allow customization.**
How to Create a Pseudo-signature

1. Users select a password
2. Decide which cues to use
3. Select cues and adjust their placement
4. Decide an order of writing cues
5. Decide an order of writing strokes
6. Customize interpretations of the visual hints
7. Complete writing

Key1, key2, key3, ...

Stroke directions, stroke speeds, solid/dashed lines, dwelling positions,...
Theoretical Password Space

1. We assume passwords are weak, so we compute # of available cues $N$ from the specifications of cues in the GUI.
2. We assume the placements for duplicate cues are equivalent and only count one.
3. We assume minimum shift for each place position is 10 (details on Slide 17), given the drawing window 760x390 and the cue dimension 130x130, then $w*h = 64x27$.

Total # of cases for pre-sketching stage: $W = \sum P(i) \times S(i)$

$P(i)$ - # of placements for i cues;
$S(i)$ - # of stroke orders for i cues;
i, j, k – in the j-th placement of i cues, there are k unique cues.
On the Usability and Security of Pseudo-signatures
Jin Chen, Daniel Lopresti,

Theoretical Password Space

1. To select k unique cues, there are \( \binom{N}{k} \) ways.
2. To place these i cues (including duplicate cues, if any) in i out of wxh cue positions, there are \( \binom{w \times h}{i} \) ways.
3. To exclude cases for duplicate cues, suppose the cue selection is as this: \( a_{j1} + a_{j2} + \ldots + a_{jk} = i \), then the \# of repetitive placements is \( w_j = a_{j1}! \times a_{j2}! \times \ldots \times a_{jk}! \). Combining 1-3:

\[
P(i) = \sum_j \left( \binom{N}{k} \times \binom{w \times h}{i} \right) \times i / w_j
\]

4. \( S(i) \) denotes the \# of combinations of stroke orders for i cues. There are one to four strokes, so \( (1i)! \leq S(i) \leq (4i)! \)
Theoretical Password Space

Note that the # of 8-bit Printable-ASCII passwords is \(95^8 \approx 2^{53}\)
Principal Usability Questions

• *Password Selection*: a common textual password.

• *Cue Selection*: any user preference about cue shape, and its location in the palette?

• *Cue Placement*: can users consistently recall?

• *Order Selection*: how to decide the writing order? How do users remember the order?

• *Sketching*: how to decide the “visual hints,” i.e., writing speed, stroke direction/format, dwelling, etc.?
Principal Security Questions

• *Password Selection*: presumably weak.

• *Cue Selection*: cue shape/location preference might hamper security.

• *Cue Placement*: how does it affect biometric keys? Are there any less secure patterns?

• *Order Selection*: how does it affect biometric keys?

• *Sketching*: any strong user preference on “visual hint?” Does population statistics help guess the sketching?

Unfortunately, we are only able to answer part of them for now.
## Experimental Design

<table>
<thead>
<tr>
<th>Round</th>
<th>Description</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round-E1</td>
<td>Password selection + Cue selection + Cue placement + Sketching completion.</td>
<td>1,870</td>
</tr>
<tr>
<td></td>
<td><em>Repeat one input for 10 times.</em></td>
<td>34 users</td>
</tr>
<tr>
<td>Round-E2</td>
<td>Password selection + Cue selection + Cue placement + Sketching completion.</td>
<td>350</td>
</tr>
<tr>
<td></td>
<td><em>One input for each cue palette.</em></td>
<td>34 users</td>
</tr>
<tr>
<td>Round-E3</td>
<td>Password selection + Cue selection + Cue placement + Sketching completion.</td>
<td>350</td>
</tr>
<tr>
<td></td>
<td><em>Repeat one input for 10 times.</em></td>
<td>34 users</td>
</tr>
</tbody>
</table>
On the Usability and Security of Pseudo-signatures
Jin Chen, Daniel Lopresti,

**Biometric Key Generator**

**Template T:**

\[
\begin{bmatrix}
\min F_1, \max F_1 \\
\min F_2, \max F_2 \\
\ldots \\
\min F_n, \max F_n
\end{bmatrix}
\]

**Offset \( \Omega \):**

\[
\begin{bmatrix}
\min F_1 \% \Delta F_1 \\
\min F_2 \% \Delta F_2 \\
\ldots \\
\min F_n \% \Delta F_n
\end{bmatrix}
\]

**Key K:**

\[
\begin{bmatrix}
\frac{F_1 - \Omega_1}{\Delta F_1} \\
\frac{F_2 - \Omega_2}{\Delta F_2} \\
\ldots \\
\frac{F_n - \Omega_n}{\Delta F_n}
\end{bmatrix}
\]

The template divides the feature space into intervals along each dimension and thus is able tolerant inputs with small variance, i.e., output the same key.
Feature Selection

A heuristic metric borrowed from Ballard, et.al. \cite{Ballard2006}:

\[ Q = \frac{a - r + 1}{2} \]

- a: percentage forgers fail to replicate
- r: percentage legitimate users fail to repeat

Sort Q-values from 121 features, then divide them into spatial and temporal features, and then filter out any feature with Q-value less than 0.6. Finally we get 16 spatial features and 8 temporal features.

Usability Issues

Preference on cue positions in the GUI (Round-E1, E2) (6.7% if equally likely chosen)

<table>
<thead>
<tr>
<th></th>
<th>Col 1</th>
<th>Col 2</th>
<th>Col 3</th>
<th>Col 4</th>
<th>Col 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row 1</td>
<td>6%</td>
<td>7%</td>
<td>6%</td>
<td>6%</td>
<td>7%</td>
</tr>
<tr>
<td>Row 2</td>
<td>6%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Row 3</td>
<td>6%</td>
<td>8%</td>
<td>9%</td>
<td>8%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Preference on cue shapes in the GUI (Round-E1, E2) (16.7% if equally likely chosen)

<table>
<thead>
<tr>
<th></th>
<th>Square</th>
<th>Triangle</th>
<th>Circle</th>
<th>X-shape</th>
<th>Z-shape</th>
<th>Arc</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14%</td>
<td>17%</td>
<td>23%</td>
<td>16%</td>
<td>11%</td>
<td>18%</td>
</tr>
</tbody>
</table>
Security Issues

• Symmetry: 15.5% samples are left-right symmetric. 374 samples from 34 users. Other symmetric patterns are much less common in our observations (Round-E1, E2).

• Cue selection and placement: 5.9% sample pairings have the same set of cues (Round-E2).
Security Issues

Influence of cue position on biometric key

![Graph showing the impact of cue position on biometric key](image)

- X:
- Y:

Impact of Cue Position on Biometric Key

- Hamming Distance of Keys
- Position Offset (x-/y- Direction)
More Facts

• 255 out of 340 pseudo-signatures are drawn in a “natural” writing style: left to right and top to bottom (Round-E1).
  -- It might due to the fact of right-handed writers.

• ~52% of the multi-stroke cues are sketched as the numeric labels indicate.
  -- It might due to the mnemonic effect of these labels.

• ~72% of dashed strokes are sketched as solid ones.
  -- It might due to habitual effect of the writers.

However, more data/experiment are needed to justify them.
Conclusion and Future Work

• Theoretical password space is much larger than textual one.
• Symmetry issue seems less severe than “DAS”.
• No salient user preferences on cue selection stage.

• Investigate the machine-based generative attacks to this multi-step procedure of creating pseudo-signatures.
• Design models to compute the practical password space.
• Design feedback mechanism in the GUI to help users create stronger pseudo-signatures.
Thank You!