Do background images improve “Draw a Secret” graphical passwords?

Jeff Yan
School of Computing Science
Newcastle University, UK
(Joint work with Paul Dunphy)

Context

- Textual passwords
  - Cheap, convenient, ubiquitous
  - Have long suffered usability problems
    - Due to limitations of human memory

- Graphical passwords
  - A picture is worth a thousand words
  - Hot topic in both security and HCI communities
  - Bonder ('96), Passfaces, Inkblot, Passpoints, etc.
  - Collective understanding: still in its infancy

“Draw a Secret” [Usenix’99]

- One representative scheme; one of the few supporting both
  - Authentication: to verify the claimed identify of a user, and
  - Key generation: to use a password to generate a long crypto key

- Theoretical password space: DAS > textual

“Draw a Secret”

- A password is a free-form drawing on a grid of size N x N
  - Sample: encoded as (2, 2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5), (1,2), (1,3), (5,5)
  - Two secrets are the same if the encoding is the same;

- Determinants of password strength include
  - Stroke count (2)
  - Password length (8)
  - Grid size (4x4)

Figure 2: Layout of a graphical password on a 4 x 4 grid. The drawing is mapped to a sequence of coordinate pairs by listing the cells in the order which the stylus passes through them, with a distinguished coordinate pair inserted in the sequence whenever the stylus is lifted from the drawing surface.
Problems with DAS

- Users tend to pick weak passwords that are vulnerable to *graphical dictionary attack* (Thorpe and van Oorschot [usenix'04])
  - Small stroke count,
  - Small password length,
  - Mirror symmetry

- Implication: this theoretically sound scheme is less secure in practice
  - 1-week recall (pilot): avg strength of memorable passwords < 41.9 bits (vs. 8-character text pwd: 53 bits)

Grid selection as a solution

- Thorpe and van Oorschot [acsac04]
- How it works:
  - Adds up to 16 bits to the password space
  - Unclear it works well as expected (no empirical study yet)

Intuition behind our solution

- In DAS, difficult to reconstruct a complex secret
  - E.g. people were able to remember what their drawings looked like, but failed to replicate them in the correct location (Goldberg et al [CHI'02])

- The cells in the grid all look alike!
  - What if recreation of a secret can be aided by something that reduces the confusion, e.g. a background image?

Our novel proposal

- Background Draw a Secret (BDAS):
  - Instead of creating a secret on an empty grid, a user choose a background image to be overlaid by the grid, and then create a secret as in DAS
Empirical evaluations

- **Design**
  - Paper/transparency prototype
  - Drawing grid
    - 5x5
    - Same size as a popular PDA
  - Comparative study
    - DAS: grid printed on transparency
    - BDAS: choose one out of 5 images to be overlaid with grid

- **Procedure**
  - 46 participants
    - 26: non-technical
    - 32 M, 14 F
    - Age: 18-25 (one 50+)
  - Briefing & randomly assigned a group
  - Practice
  - Password creation
  - 5-minute recall
  - 1-week recall

What background image to choose?

- Little guideline in literature
- have meaningful content and rich details (Wiedenbeck et al SOUPS'05)
- Easy to select spots
- Intuition
  - Not introduce obvious bias
  - Everyday images

Background images used

- Stars
- Map
- Plant
- Crowds
- Playing card
  - Low-detail

Results: background image choice

- Images dense with content (map and crowd) anticipated to be the most popular
  - This was clearly contradicted
  - Playing card: 33% of selections, plant: 30%
Results: password quality

- Complexity of secrets in each group
  - BDAS: larger stroke count (significantly different) and password length
  - BDAS: stronger by more than 10 bits
- Symmetry: 43% (BDAS) vs 57% (DAS)
- Centering within the grid: 43% (BDAS) vs. 87% (DAS)

<table>
<thead>
<tr>
<th>Group</th>
<th>Strokes</th>
<th>Password length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avg.</td>
<td>S.d.</td>
</tr>
<tr>
<td>BDAS</td>
<td>7.22</td>
<td>2.21</td>
</tr>
<tr>
<td>DAS</td>
<td>5.30</td>
<td>2.44</td>
</tr>
</tbody>
</table>

Results: 5-minute recall

- Recall rate
  - DAS: 100% (23/23); BDAS: 96% (22/23) [Fig10(a)]
- Complexity of successfully recalled secrets:
  - BDAS: larger stroke count (significantly different) and password length; avg strength: larger by more than 10 bits
  - BDAS: less symmetry and centering

<table>
<thead>
<tr>
<th>Group</th>
<th>Strokes</th>
<th>Password length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avg.</td>
<td>S.d.</td>
</tr>
<tr>
<td>BDAS</td>
<td>7.45</td>
<td>2.26</td>
</tr>
<tr>
<td>DAS</td>
<td>5.30</td>
<td>2.44</td>
</tr>
</tbody>
</table>

Results: 1-week recall

- Recall rate
  - DAS = BDAS = 95% (20/21)
- Complexity of successfully recalled secrets:
  - BDAS: larger stroke count (significantly different) and password length
  - Avg strength: <60 bits (DAS); >70.2 bits (BDAS)
  - BDAS: less symmetry and centering

<table>
<thead>
<tr>
<th>Group</th>
<th>Strokes</th>
<th>Password length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avg.</td>
<td>S.d.</td>
</tr>
<tr>
<td>BDAS</td>
<td>7.1</td>
<td>2.16</td>
</tr>
<tr>
<td>DAS</td>
<td>5.2</td>
<td>2.44</td>
</tr>
</tbody>
</table>

Summary

- A simple idea: introducing background images into DAS
- Nice results
  - Much stronger passwords; just as memorable as their much simpler DAS counterparts.
  - The most exciting bit: A simple idea significantly enhances both usability and security simultaneously
- Numerous possibilities for future study
Ongoing and future work

- Larger scale of experiments with an actual implementation
  - DAS vs. BDAS
  - BDAS vs. textual passwords
- What will make good background images?
  - Effect of individual background image choices
- Shoulder surfing resistance
- Interference between multiple passwords
- Many more ...

Thank You!

Jeff.Yan@ncl.ac.uk