Graphical Passwords (2)
Categories

- picture/photo based vs. grid based
- recognition based vs. recall based
Usability concerns

- **Usability**
  - Are the passwords easy to memorize?
  - Is the authentication process simple?
  - Is it easy to input the password?
  - How long does it take to input the password?
Security concerns

Security

- Is the password scheme resistant to various attacks?
  - Brute force
  - Educated guess
    - Collective educated guess
    - Individualized educated guess
  - Shoulder surfing
  - Spyware
  - Social engineering
Educated Guess Resistant
Graphical Password Schemes
Déjà Vu [Dhamija+00]

- Picture based / recognition based
  - Use random images generated by Andrej Bauer’s *Random Art*

- Three phases:
  - portfolio creation
  - training
  - authentication
Déjà Vu – Sample Screenshot
Déjà Vu – Usability

- Memorability
  - Their user study suggests the portfolios are much easier to remember than the textual passwords
  - However, the study is limited (only 20 participants)
  - Quantitative result

<table>
<thead>
<tr>
<th></th>
<th>PIN</th>
<th>Password</th>
<th>Art</th>
<th>Photo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Logins</td>
<td>5% (1)</td>
<td>5% (1)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Failed Logins (after one week)</td>
<td>35% (7)</td>
<td>30% (6)</td>
<td>10% (2)</td>
<td>5% (1)</td>
</tr>
</tbody>
</table>

Table 2: % Failed logins (# failed logins/20 participants)

- Qualitative result

Although some users remarked that they would never be able to remember the portfolios they created, all were surprised that they could recognize their images and at how quickly the selection took place.
Déjà Vu – Usability

- Random Art vs. Photo?
  - Resistance to educated guess attack vs. memorability

- Authentication process
  - It takes a significant time for portfolio creation + training
  - Takes more time to input the password compared to the textual passwords

<table>
<thead>
<tr>
<th></th>
<th>PTN</th>
<th>Password</th>
<th>Art</th>
<th>Photo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>60</td>
</tr>
<tr>
<td>Login</td>
<td>15</td>
<td>18</td>
<td>32</td>
<td>27</td>
</tr>
<tr>
<td>Login (after one week)</td>
<td>27</td>
<td>24</td>
<td>36</td>
<td>31</td>
</tr>
</tbody>
</table>

Table 1: Average seconds to create/login
Déjà Vu – Security

- Password space

\[ \binom{n}{k} \], where \( n \) is the # of images in the challenge set and \( k \) is the # of portfolio images shown.

- e.g. if \( n = 20 \) and \( k = 5 \), the space size = 15504 (slightly bigger than that of 4-digit PIN)

- The image generating seed value should be stored in the authentication server unencrypted

- Resistant to educated guess attacks

- May be vulnerable to
  - brute force
  - shoulder surfing
Use your illusion

- Below are three distorted images
  Can you guess what the original photos represent?
Use your illusion

Lorrie Cranor

Hunt Library

River & Bridge (my wallpaper)
Use your illusion [Hayashi+08, 11]

- [https://arima.okoze.net/illusion/](https://arima.okoze.net/illusion/)
- Photo based / recognition based
  - A user has to upload 3 of his/her own images and memorize the *distorted images* of those as the portfolio
Use your illusion – Usability

- Memorability
  - Easier to remember because the user chooses her own images

<table>
<thead>
<tr>
<th></th>
<th>The 1st day</th>
<th>2 days later</th>
<th>1 wk. later</th>
<th>4 wks. later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-selected, non-distorted</td>
<td>100%(18)</td>
<td>100%(18)</td>
<td>100%(18)</td>
<td>100%(18)</td>
</tr>
<tr>
<td>Self-selected, distorted</td>
<td>100%(18)</td>
<td>100%(18)</td>
<td>100%(18)</td>
<td>100%(18)</td>
</tr>
<tr>
<td>Imposed, distorted</td>
<td>100%(18)</td>
<td>89%(16)</td>
<td>94%(17)</td>
<td>89%(16)</td>
</tr>
</tbody>
</table>

- Login Time

<table>
<thead>
<tr>
<th></th>
<th>1st day</th>
<th>2 days later</th>
<th>1 wk. later</th>
<th>4 wks. later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-selected, non-distorted</td>
<td>11.5 (9.9)</td>
<td>12.3 (12.3)</td>
<td>12.7 (11.9)</td>
<td>12.5 (12.8)</td>
</tr>
<tr>
<td>Self-selected, distorted</td>
<td>12.4 (11.2)</td>
<td>16.4 (15.9)</td>
<td>14.3 (13.4)</td>
<td>17.9 (16.5)</td>
</tr>
<tr>
<td>Imposed, distorted</td>
<td>16.7 (14.1)</td>
<td>25.8 (19.0)</td>
<td>25.1 (17.6)</td>
<td>24.7 (16.7)</td>
</tr>
</tbody>
</table>
Password space
- The same formula as that of Déjà Vu scheme
- If $n = 27$ and $k = 3$, the space size $= 2925$

Resilient to educated guess attacks

May be vulnerable to
- Brute force attacks
- Shoulder surfing
Brute Force Search Resistance
Graphical Password Schemes
Previous two schemes have relatively small password space under their default settings
- Déjà Vu: 15504 (where $n = 20$, $k = 5$)
- Use your illusion: 2925 (where $n = 27$, $k = 3$)

We can tune the variables $n$ and $k$ to enlarge the password space

Then how about the usability??
- It would be more tedious to look at so many pictures if the # of all images shown in a challenge set ($n$) gets bigger
- Trade-off between password space and usability
Draw-A-Secret (DAS) [Jermyn+99]

- Grid based / recall based scheme

(a) User inputs desired secret

(b) Internal representation
Memorability

- Not all the available passwords are memorable but there are some categories of passwords that are relatively memorable
  - Simple shapes, letters, ...
  - Patterns that can be generated by short algorithms
  - Symmetric patterns

Easy to input?

- Suitable for the touch devices (e.g. PDAs, smartphones)
- Somewhat difficult with mouse

Not enough user studies about the usability
Large enough password space with 5x5 grid

When $L_{\text{max}} > 11$, the space size surpasses that of textual password with 8 characters ($95^8 \approx 2^{53}$)

This is true in theory, but how about in reality?

- People tent to choose memorable patterns (e.g. symmetric patterns)
- Vulnerable to collective educated guess attacks (just like dictionary attacks of textual passwords)

Table 1: Number of passwords of total length less than or equal to $L_{\text{max}}$ on a $5 \times 5$ grid.
A DAS Variant in real life

- Android phone unlock patterns
Android unlock patterns

- Usability
  - Any ideas? Want to hear from the actual users.

- Security
  - Password space
  - How about the smudges on the touch screen?

<table>
<thead>
<tr>
<th>N</th>
<th># of PINs</th>
<th># of patterns (unrestricted)</th>
<th># of patterns (restricted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>100</td>
<td>56</td>
<td>56</td>
</tr>
<tr>
<td>3</td>
<td>1,000</td>
<td>360</td>
<td>304</td>
</tr>
<tr>
<td>4</td>
<td>10,000</td>
<td>2,280</td>
<td>1,400</td>
</tr>
<tr>
<td>5</td>
<td>100,000</td>
<td>14,544</td>
<td>5,328</td>
</tr>
<tr>
<td>6</td>
<td>1,000,000</td>
<td>92,448</td>
<td>16,032</td>
</tr>
<tr>
<td>7</td>
<td>10,000,000</td>
<td>588,672</td>
<td>35,328</td>
</tr>
<tr>
<td>8</td>
<td>100,000,000</td>
<td>3,745,152</td>
<td>49,536</td>
</tr>
</tbody>
</table>

Numbers obtained from http://playingwithmodels.wordpress.com/2010/04/14/andoid_unlock_patterns/
Is a small password space *always* bad?

- Any ideas?
All of the previously mentioned graphical password schemes are vulnerable to...?
Shoulder Surfing Resistant Graphical Password Schemes
- Picture based / recognition based scheme
  - A user selects $k$ pass-objects (portfolio)
  - Then the user has to click somewhere inside the convex hull of the pass objects
  - To prevent from random guessing, the user is required to do repeat this challenge a few times (e.g. 10 times)
Convex Hull Scheme – Usability

- No formal user study for this scheme

- Memorability
  - Would be similar to that of Déjà Vu

- Authentication process
  - To make this scheme effective, the value $n$ should be big enough $\rightarrow$ difficult to find the pass-objects
  - Unlike the Déjà Vu / Use your illusion schemes, the user is required to find all the $k$ pass-objects together to see the invisible convex hull, which might affect the usability
Convex Hull Scheme – Security

- Password space

“The number of possible passwords is the "binomial coefficient" (choose any $K$ objects among $N$). **When $N = 1000$ and $K = 10$,** the number of possible passwords is hence approximately $2.6 \times 10^{23}$. This is a little more than the number of alpha-numeric passwords of length 15 ($36^{15} \approx 2.2 \times 10^{23}$). Having $N = 1000$ objects is not unreasonable (compare with the "Where is Waldo" puzzles, where there are typically tens of thousands of little persons in a picture).”

- Maybe true, but no evidence

- Resistant to shoulder surfing attack
Summary – Characteristics of Graphical Passwords
Usability of graphical passwords

- More memorable than textual passwords
- Takes significantly longer time to create the graphical passwords
- Takes longer time to input the passwords
- More restrictions
  - big enough screen size is often required
  - some schemes require extra devices (e.g. touch screen)
Memorability

Why is it so important to make more memorable password schemes?
- One of the most important problems of textual passwords

Are the graphical passwords really significantly more memorable?
- We do not know yet
- We need to conduct larger scale field studies
What if a user has many graphical passwords? Would it be still easy enough to correctly remember all of them?

- Chiasson et al. suggest that it may not be the case

<table>
<thead>
<tr>
<th></th>
<th>No Interference</th>
<th>Interference</th>
<th>$\chi^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confirm</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool</td>
<td>139/284 (49%)</td>
<td>63/99 (64%)</td>
<td>$\chi^2 (1, N=383)=6.36, p&lt;.05$</td>
</tr>
<tr>
<td>Cars</td>
<td>108/193 (56%)</td>
<td>62/100 (62%)</td>
<td>n.s.</td>
</tr>
<tr>
<td><strong>Login</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool</td>
<td>1224/1541 (79%)</td>
<td>226/319 (71%)</td>
<td>$\chi^2 (1, N=1860)=11.33, p&lt;.001$</td>
</tr>
<tr>
<td>Cars</td>
<td>1053/1216 (87%)</td>
<td>248/347 (71%)</td>
<td>$\chi^2 (1, N=1563)=44.26, p&lt;.001$</td>
</tr>
</tbody>
</table>
Security of graphical passwords

- Security and usability trade-off
- Resistant to...
  - Dictionary attacks
  - Social engineering (e.g. phishing)
- Vulnerable to...
  - Brute force attacks
  - Educated guess attacks
  - Shoulder surfing
- How about the spywares?
Authentication server’s concerns

- Usually needs more space than the textual passwords
- The passwords cannot be easily hashed
How should we embrace the graphical passwords?

- Quick poll
  - How many of you would like to try out some of the graphical passwords?
  - How many of you would like to use the graphical passwords as your main password scheme?

- How should we embrace them?
Conclusion
Graphical passwords and textual passwords have different characteristics.

Graphical passwords are good for authentication, but not as much good for key generation in general.

There exist various graphical password schemes, each with its own strengths and weaknesses.

More user studies with focus on “usability” are needed.
- Memorability is not the only usability concern.
References


Questions?
Related topic

- Social CAPCHA of Facebook