
Presented By: Miss Samya Ashraf Want
Student ID- 24446467

saw2g10@ecs.soton.ac.uk
Contents

- Use of Passwords
- What is an Ideal Password?
- Password Schemes
- Example and drawbacks of earlier schemes
- Color login
- Improvisation & Conclusion
Use of Passwords

- Required for authenticating, in order to provide access to something (resource, object).

Password

Authentication

Providing access
What is an Ideal Password?

- Easy to remember
- Difficult to guess
- Reduces login time

Ideal Password
Password Schemes

- Alphanumeric password
- Graphical password
- Biometric password
Drawbacks of Alphanumeric and Biometric schemes

- Alphanumeric
  - Passwords can either be easily remembered or difficult to guess but not both.
  - Vulnerable to shoulder surfing.
- Biometric
  - Expensive to build additional devices for authenticating user’s physical characters.
  - Increased login time.
  - Fear of the entire device becoming useless incase of a surgery or an accident changing the biometric feature.
Idea Of Graphical Password Schemes

- Recognition is easier than recall.
  “I know you but I forgot your name”

Conaughey  Ventimiglia
Types Of Graphical Passwords Schemes

- Recognition based
- Recall based
Examples and Drawbacks of Earlier Graphical Password Schemes

- Deja Vu does not fully satisfy the condition that the passwords are easier to remember.
- Passfaces, where human faces are used as passwords is not efficient due to the limitation of candidate faces on screen.
- Convex Hull makes the screen crowded making it difficult for the user to identify the password icon.
Colorlogin

- Recognition based graphical password
- The image background color is used as a safety factor
- Allows the user to click on a deceptive icon instead of a password icon.
Design Of Colorlogin

• Initially the user selects an image background color and the password icons.
• During authentication process, user concentrates only on the predefined background color since that contains the password icon amongst other background color icons.
• There are four security levels called low, medium, high and self-define, where,
  \[ \text{Level of Security} \propto \text{No. of Colors} \]
• Therefore the workload is reduced.
An example of icons displayed during authentication using colorlogin
The Display Screen after the user clicks on the rows containing the password icon
Advantages of colorlogin

- Overcomes the weakness associated with mouse-click dependent schemes and therefore is resistant to shoulder surfing.
- Reduces workload.
- Sufficient password space as compared to other graphical password schemes.

<table>
<thead>
<tr>
<th>C, k, Nc</th>
<th>3, 3, 40</th>
<th>4, 4, 72</th>
<th>5, 5, 112</th>
</tr>
</thead>
<tbody>
<tr>
<td>space</td>
<td>3e+5</td>
<td>4e+7</td>
<td>6e+9</td>
</tr>
</tbody>
</table>

C- No. of colors used, k- No. of pass-icons, Nc- No. of total icons per color for different value of C
Mean times (seconds) of 30 participants for 5 correct logins

<table>
<thead>
<tr>
<th>R (No. of rounds for authentication)</th>
<th>Grid size of Colorlogin</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9*9</td>
<td>12*12</td>
<td>15*15</td>
<td></td>
</tr>
<tr>
<td>R=1</td>
<td>3.4</td>
<td>5.2</td>
<td>5.5</td>
<td></td>
</tr>
<tr>
<td>R=2</td>
<td>8.2</td>
<td>9.6</td>
<td>11.2</td>
<td></td>
</tr>
<tr>
<td>R=3</td>
<td>11.3</td>
<td>13.6</td>
<td>15.2</td>
<td></td>
</tr>
</tbody>
</table>
Improvisation and Conclusion

- Taking the security mechanisms to a higher level.
- Improving measures to reduce the login time.
- The fact that personality could predict color creating hotspots should be considered.
- The color-blind users should be taken into account.
THANK YOU