A Graphical Password Authentication System

Presented by........

Ch.Satish
(08F01A0518)
Abstract

Graphical passwords provide an alternative view to traditional alphanumeric passwords.

In this extended abstract, propose a simple graphical password authentication system. It describes operation with some examples, and highlight important aspects of the system.
Introduction

- Use textual passwords augmented by some graphical capabilities

- They are attractive since people usually remember pictures better than words

- Also, they should be more resistant to brute-force attacks, since the search space is practically infinite.
Identification

Possession ("something I have")
- Key Passport
- Smart Card

Biometrics ("something I am")
- Face
- Fingerprint
- Iris

Knowledge ("something I know")
- Password
- PIN
Passwords: method of choice for user authentication

 Usually it is 8-15 character or slightly more than that

 Ten years back Klein performed such tests and he could crack 10-15 passwords per day.

 Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play.
Passphrase

- It’s nothing but the enhance version of password.
- Usually it is a combination of words or simply collection of password in proper sequence is passphrase.
- Length of passphrase is about 30-50 character or more than that also.
- 30-50 character is creates ambiguity to remember if there is no any proper sequence.
Biometrics

- Refer to a broad range of technologies
- Automate the identification or verification of an individual
- Based on human characteristics or body organs
  - Physiological: Face, fingerprint, iris
  - Behavioral: Hand-written signature, voice

Characteristics Templates

011001010010101...
011010100100110...
001100010010010...
Graphical password

- Used for any devices with graphical input display
- Primarily for PDAs: Palm Pilot, HP iPAQ, …
Observation

- Textual password input via keyboard
  - simplepas
  - 12345679
- Graphical password
TEXT WITH GRAPHICAL ASSISTANCE

GRAPHICAL PASSWORD

TEXTUAL PASSWORD WITH GRAPHICAL ASSISTANCE

DRAW-A-SECRET SCHEME
Example: password is "tomato".

Usual way of input:

```
0. _ _ _ _ _ _
1. t _ _ _ _ _
2. t o _ _ _ _
3. t o m _ _ _
4. t o m a _ _
5. t o m a t _
6. t o m a t o
```

Conventional.
With graphical assistance

(a) Left-to-right

(b) Rotated left

(c) Outside-in

(d) A more complex example
DRAW-A-SECRET (DAS) SCHEME

- Password is picture drawn on a grid.
- Users are freed from having to remember an alphanumeric string.
- What is good about picture-based password?
Encryption Tool for PDA

- Use **Triple-DES** to encrypt/decrypt data stored on PDA

  - Sequence of coordinates of password \( P \)
  - Hashed using SHA-1
  - Key \( k \)
  - Derived to make keys
  - Triple-DES
Encryption Tool for PDA

Process of setting password

Sequence of coordinates $P$

Hashed using SHA-1

Key $k$

$E_k(P)$

Store $E_k(P)$

Process of verifying password

Sequence of coordinates $P’$

Hashed using SHA-1

Key $k’$

result = $D_{k’}(E_k(P))$

result = $P$ ??
Size of Password space

\[ \Pi(L_{\text{max}}, G) = \sum_{L=1}^{L_{\text{max}}} P(L, G) \quad \text{Grid size } G \times G \]

\[ P(L, G) = \sum_{l=1}^{L} P(L-1, G)N(I_G) \quad l : \text{length of stroke} \]

\[ N(1, G) = \sum \text{n}(x, y, l, G) \quad n : \text{number of strokes} \]

\[ (x, y) \in [1..G] \times [1..G] \quad (x, y) : \text{ending cell} \]
DRAW-A-SECRET (DAS) SCHEME

<table>
<thead>
<tr>
<th>$L_{\text{max}}$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>log$_2$(# passwords)</td>
<td>5</td>
<td>10</td>
<td>14</td>
<td>19</td>
<td>24</td>
<td>29</td>
<td>33</td>
<td>38</td>
<td>43</td>
<td>48</td>
</tr>
<tr>
<td>$L_{\text{max}}$</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>log$_2$(# passwords)</td>
<td>53</td>
<td>58</td>
<td>63</td>
<td>67</td>
<td>72</td>
<td>77</td>
<td>82</td>
<td>87</td>
<td>91</td>
<td>96</td>
</tr>
</tbody>
</table>

Table 1: Number of passwords of total length less than or equal to $L_{\text{max}}$ on a 5 x 5 grid.

However, above table shows **raw** size of graphical password space **surpasses** that of textual passwords.
To login, user is required to click within the circled red regions (chosen when created the password) in this picture. The choice for the four regions is arbitrary.
CONCLUSION:

- In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.
References:

- “The Design and Analysis of Graphical Passwords” by Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K.Reiter, Aviel D.Rubin
- “Graphical passwords” by Leonardo Sobrado, Jean-Camille Birget, Department of Computer Science, Rutgers University
- “Graphical Dictionaries and the Memorable Space of Graphical Passwords” by Julie Thorpe, P.C. van Oorschot
- “Human Memory and the Graphical Password” by David Bensinger, Ph.D.
Thank you!
ANY QUERIES...????