Graphical Passwords

Jaanus Kase, jkase@andrew.cmu.edu
05-899 Usable Privacy and Security, Spring 2008
Outline

• Why are graphical passwords (GP) interesting?
• Theory of password use
• GP security properties
• Types of GP
• Examples and analyses
• Demos
• (bonus from CHI2008)
Exercise time :-}
Meet a couple of new classmates

Glatik

Brimol

Exercise material adapted from 05-610 HCI Methods.
Do you have trouble remembering names?

• Heard people say this?
  “I can’t remember names but I never forget a face.”

• Is this statement accurate? If so, why is it so?
Remember the face you saw on the right?

Draw it
Score your memory

1 point each for

- Round head
- Eyes wide apart
- Big straight nose
- Heart-shaped lips
- Dimple in chin

Your score:
0? 1-2? 3-4? 5?
Do you remember the names?
Write down the two names

- Glimok
- Brimol
- Bratik
- Glatik

Your score?

Exercise material adapted from 05-610 HCI Methods.
What’s happening? Aren’t faces easier to remember?

- Why were the names easier to remember?
  - Was this little demonstration different from remembering names or faces typically?

- Typically:
  - You recall names & recognize faces

- In this demonstration:
  - You recalled faces & recognized names

Exercise material adapted from 05-610 HCI Methods.
Recognition vs recall

• A key HCI principle for (GUI) interfaces:

  **Recognition is easier than recall**

• Many graphical password schemes capitalize on this in different ways
Outline

• Why are graphical passwords (GP) interesting?
  • Theory of password use
  • GP security properties
  • Types of GP
  • Examples and analyses
  • Demos
Why are graphical passwords interesting?

- Picture Superiority Effect
  - Dual coding theory
- Recognition is easier than recall
- Text passwords are hard to remember
  - Human memory not “built” for precise recall
Outline

• Why are graphical passwords (GP) interesting?

• **Theory of password use**

• GP security properties

• Types of GP

• Examples and analyses

• Demos
Password uses

- Authentication
  - Output is one bit, "yes" or "no"
- Key generation
  - "Seed" for a crypto key generator
  - 80+ bits needed
  - Graphical passwords are not strong enough for this
Outline

- Why are graphical passwords (GP) interesting?
- Theory of password use
- **GP security properties**
- Types of GP
- Examples and analyses
- Demos
Security properties of graphical passwords

• Often based on filtering, aggregation and tolerance windows

• Too little entropy for key generation

• Resistant against some attacks

• Shoulder surfing

• Sharing, social engineering (pretexting)

• In-place training required to remember
Outline

• Why are graphical passwords (GP) interesting?
• Theory of password use
• GP security properties
• **Types of GP**
• Examples and analyses
• Demos
Graphical password types

- Pure recall
  - Draw-a-Secret (DAS)
- Cued recall
  - Blonder, Background-DAS, visKey, PassPoints and other click-point systems
- Recognition
  - (SiteKey,) Passfaces, Déjà vu
Outline

• Why are graphical passwords (GP) interesting?
• Theory of password use
• GP security properties
• Types of GP
• **Examples and analyses**
• Demos
Blonder patent

- U.S. patent 5,559,961
- Filed 1995, issued 1996
- Describes graphical password entry as used by the cued recall systems that use sequence of points
- Unclear if has prevented commercial deployments
- Patents cited as hindrance in keystroke authentication reading chapter
“Draw-a-Secret”

- Draw a simple picture on a 2D grid
- Counts edge crossings and “used” squares in grid
Passfaces

- Select passfaces from a set of faces (3x3 grid, 1 correct, 8 fakes)
- “Facebook edition”
- Security?
visKey / visKeeper

- Application to store bank account details, passwords, contacts, and other private info
- Click on hotspots in a given order
- User-definable tolerance
- Claims to encrypt data, but where does the key come from?
Security: shoulder surfing

Table 1. Real and Perceived Vulnerability Descriptive Statistics, ANOVA and Duncan’s Multiple Range Test Results

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Average</th>
<th>Std. Dev.</th>
<th>Duncan Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Dictionary Password</td>
<td>3.65</td>
<td>1.631</td>
<td>A</td>
</tr>
<tr>
<td>PassFaces with Mouse</td>
<td>3.1</td>
<td>1.119</td>
<td>A</td>
</tr>
<tr>
<td>Dictionary Password</td>
<td>1.3</td>
<td>0.923</td>
<td>B</td>
</tr>
<tr>
<td>PassFaces with Keyboard</td>
<td>0.55</td>
<td>0.510</td>
<td>C</td>
</tr>
</tbody>
</table>

ANOVA: $F = 34.14$, $p$-value $< 0.001$, items with the same letter are not significantly different in Duncan’s Multiple Range Test.

System being Vulnerable to Shoulder-surfing Attacks (1=Not Vulnerable at All, 7=Extremely Vulnerable)

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Average</th>
<th>Std. Dev.</th>
<th>Duncan Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>PassFaces with Mouse</td>
<td>5.2</td>
<td>1.005</td>
<td>A</td>
</tr>
<tr>
<td>Non-Dictionary Password</td>
<td>5.05</td>
<td>0.945</td>
<td>A</td>
</tr>
<tr>
<td>Dictionary Password</td>
<td>4.85</td>
<td>1.309</td>
<td>A</td>
</tr>
<tr>
<td>PassFaces with Keyboard</td>
<td>2.3</td>
<td>1.129</td>
<td>B</td>
</tr>
</tbody>
</table>

ANOVA: $F = 30.90$, $p$-value $< 0.001$, items with the same letter are not significantly different in Duncan’s Multiple Range Test.

Table 2. Participant Opinions on Recording of the Authentication Information Descriptive Statistics, ANOVA and Duncan’s Multiple Range Test Results

How Easy it is to Record the Passwords/Passfaces (1=Extremely Difficult, 7=Extremely Easy)

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Average</th>
<th>Std. Dev.</th>
<th>Duncan Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>PassFaces with Mouse</td>
<td>5.2</td>
<td>1.196</td>
<td>A</td>
</tr>
<tr>
<td>Non-Dictionary Password</td>
<td>5.05</td>
<td>1.234</td>
<td>A</td>
</tr>
<tr>
<td>Dictionary Password</td>
<td>2.45</td>
<td>1.191</td>
<td>B</td>
</tr>
<tr>
<td>PassFaces with Keyboard</td>
<td>1.6</td>
<td>0.754</td>
<td>C</td>
</tr>
</tbody>
</table>

ANOVA: $F = 53.86$, $p$-value $< 0.001$, items with the same letter are not significantly different in Duncan’s Multiple Range Test.

How Easy it is for Hackers to Obtain Passwords/Passfaces (1=Extremely Difficult, 7=Extremely Easy)

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Average</th>
<th>Std. Dev.</th>
<th>Duncan Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary Password</td>
<td>6.7</td>
<td>0.47</td>
<td>A</td>
</tr>
<tr>
<td>Non-Dictionary Password</td>
<td>5.65</td>
<td>0.875</td>
<td>B</td>
</tr>
<tr>
<td>PassFaces with Mouse</td>
<td>3.95</td>
<td>1.468</td>
<td>C</td>
</tr>
<tr>
<td>PassFaces with Keyboard</td>
<td>2.75</td>
<td>1.118</td>
<td>D</td>
</tr>
</tbody>
</table>

ANOVA: $F = 56.17$, $p$-value $< 0.001$, items with the same letter are not significantly different in Duncan’s Multiple Range Test.
Click point tolerance and image choice

- Trial with 10x10, 14x14 tolerance squares
  - 10x10 was fine
- Few significant differences between different images
  - ... but different images have different number of “hotspots”, affecting security
Background Draw a Secret (BDAS)

- DAS grid + background image
- BDAS passwords 10 bits more complicated than DAS
- User drawings in BDAS group show:
  - increased complexity
  - reduced reliance on global symmetry
  - reduced reliance on centering drawings
BDAS: image choices

Figure 5. Background images used in the experiment (all reduced in size for this paper) (Map image reproduced with permission from Collins Bartholomew)

Figure 6. The distribution of background image choices (Study 1)

BDAS: memory decay

Figure 11. Memory decaying (a) the first creation (b) a week later.

Figure 12. Memory decaying (a) the first recall (b) a week later.
Multiple graphical passwords

Table 10: Effect of interference on success rate$^1$ (field)

<table>
<thead>
<tr>
<th></th>
<th>No Interference</th>
<th>Interference</th>
<th>$\chi^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confirm</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></td>
<td>Login</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>

Modeling user choice with image analysis

Outline

• Why are graphical passwords (GP) interesting?
• Theory of password use
• GP security properties
• Types of GP
• Examples and analyses

• Demos
Application demos

- visKeeper
- Passfaces Personal (Windows)
- Passfaces on web
Bonus

- Undercover: Authentication Usable in Front of Prying Eyes
- A separate visible and hidden challenge

Figure 5. Haptic device and associated machinery. The authentication system software, hosted on an external PC (not shown), pilots two servo motors that in turn govern the trackball movement.
Figure 7. Map shown to the users to explain how each position on the screen maps to a different button, depending on the trackball movement. The center position corresponds to the “vibrate” mode.
Figure 6. Visual channel. Users proceed through a series of seven challenges. The current challenge is zoomed in. Users are asked to identify which, if any, of the four pictures belong to their portfolio. The fifth ("NO") symbol is used when none of the pictures are the user’s.
Graphical Passwords

Jaanus Kase, jkase@andrew.cmu.edu
05-899 Usable Privacy and Security, Spring 2008