Give Me Letters 2, 3 and 6!
Partial Password Implementations and Attacks

David Aspinall, University of Edinburgh, UK
Mike Just, Glasgow Caledonian University, UK

Financial Cryptography and Data Security, April 2013
Outline

Partial Passwords

Survey

Guessing Attacks

Recording Attacks

Summary
Partial Passwords
Definitions and examples

A **partial password** is a challenge on a subset of characters from a full password.

A **partial password scheme** is an authentication system using partial passwords.
**Scheme**

**Registration** User chooses a password of $n$ characters from a set of $N$

**Login** Challenge of $m$ positions with response:

<table>
<thead>
<tr>
<th>Positions:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>User password:</td>
<td>a</td>
<td>s</td>
<td>h</td>
<td>u</td>
<td>f</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Correct response:</td>
<td>s</td>
<td>h</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Retry** In case of failure, user challenged again. Number of retries usually limited.

**Repeat** On next login, challenge changes.
Motivations

Introduced for telephone banking: single observation by operator does not reveal whole secret.

Online, appears to impede several attacks:

- shoulder surfing
- key logging
- man-in-the-browser

Potentially, may also thwart:

- phishing
- offline attacks

Other attractions:

- easy extra authentication step (but not true 2FA)
- cheap (e.g., compared to hardware tokens)
Origins

In UK banking: first introduced for telephone banking.

Matsumoto and Imai, _Human Identification Through Insecure Channel_ (Eurocrypt ’91). Related but more elaborate scheme:

- User has a password with known character set
- Challenge: word surrounded by detractor characters
- Response: *substituted* positions and detractors

Repeated several times.

Following work (e.g., Hopper & Bloom 2001): revised schemes and stronger guarantees, but showed required human computation steps are impractical.

So what about schemes actually in use?
Questions

- What are the security assumptions behind current deployment of partial passwords?
- What are good choices for the system parameters: password length, character set size, challenge size?
- How many observations does an attacker need to learn whole password or answer next challenge?
- Are weak passwords such as dictionary words safe?
- Failure mode: should the challenge be changed after failed attempts?
- Are some challenge sequences better than others?
- How usable is the scheme?
Survey
Online banking survey: results

- Used widely in banks, online and telephone
- Elsewhere: credit cards, utilities, outside UK, . . .
- Usually part of a multi-stage authentication, alongside: names, user ids, account details, personal knowledge questions.
- Challenge sizes fixed, vary from 2-3 positions
- Challenge sequences appear random
- Mostly: ascending position challenges, no repeats
- Most repeat same challenge on retry
- Policies generally weaker than for full passwords
<table>
<thead>
<tr>
<th>Institution</th>
<th>$N$</th>
<th>$n$</th>
<th>$m$</th>
<th>Second Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooperative</td>
<td>10</td>
<td>4</td>
<td>2</td>
<td>question</td>
</tr>
<tr>
<td>ING DiBa (DE)</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>PIN</td>
</tr>
<tr>
<td>Tesco</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>password</td>
</tr>
<tr>
<td>Smile</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>question</td>
</tr>
<tr>
<td>Nationwide</td>
<td>10</td>
<td>6</td>
<td>3</td>
<td>password</td>
</tr>
<tr>
<td>AIB</td>
<td>10</td>
<td>5</td>
<td>3</td>
<td>question</td>
</tr>
<tr>
<td>B. of Ireland (IE)</td>
<td>10</td>
<td>6</td>
<td>3</td>
<td>date of birth</td>
</tr>
<tr>
<td>Nat West, step 1</td>
<td>10</td>
<td>4</td>
<td>2</td>
<td>pp, step 2</td>
</tr>
<tr>
<td>Nat West, step 2</td>
<td>36</td>
<td>6–20</td>
<td>3</td>
<td>pp, step 1</td>
</tr>
<tr>
<td>HBoS</td>
<td>36</td>
<td>6–15</td>
<td>3</td>
<td>password</td>
</tr>
<tr>
<td>3DSecure, Boll</td>
<td>36</td>
<td>8–15</td>
<td>3</td>
<td>credit card #</td>
</tr>
<tr>
<td>Standard Life</td>
<td>36</td>
<td>8–10</td>
<td>3</td>
<td>none</td>
</tr>
<tr>
<td>Skipton</td>
<td>36</td>
<td>8–30</td>
<td>3</td>
<td>question</td>
</tr>
<tr>
<td>First Direct</td>
<td>36</td>
<td>6–30</td>
<td>3</td>
<td>question</td>
</tr>
<tr>
<td>Barclays</td>
<td>52</td>
<td>6–8</td>
<td>2</td>
<td>PIN</td>
</tr>
<tr>
<td>HSBC (CA)</td>
<td>62</td>
<td>8</td>
<td>3</td>
<td>question</td>
</tr>
</tbody>
</table>

NB: snapshot from Sept. 2012. Thanks to Atif Hussain for help with survey.
Guessing Attacks
Mode of attack for guessing

- online attack against each account
- suppose a fixed number of attempts allowed: $\beta$
- some background (e.g., dictionary), ideally limited
- no use of previous observations
- “trawling”: use best strategy on many accounts

Two typical instances of scheme:

**6 digit PIN**
- $N=10, \ n=6 \ m=2, \ \beta=6$

**8 character alphanumeric**
- $N=36, \ n=8, \ m=3, \ \beta=10$
Guessing methods

1. brute-force (sample from uniform distribution)
2. position-letter frequency (ranked list per position)
3. \textbf{projection dictionary} (ranked list per challenge)
4. dependent projection (tree per challenge) \textit{[later]}

Generate background tables by computation on:

- ordinary dictionary, e.g., /usr/share/dict/words
- dictionary with frequencies, e.g., RockYou

We calculate $\beta$-success rate: proportion of answers covered by the top $\beta$ guesses.
Example projection dictionary attack

<table>
<thead>
<tr>
<th>Challenge 2 3 6: Cum.%</th>
<th>Challenge 1 2 3: Cum.%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. a s o</td>
<td>1. i l o</td>
</tr>
<tr>
<td>2. l o y</td>
<td>2. p a s</td>
</tr>
<tr>
<td>3. r i e</td>
<td>3. m a r</td>
</tr>
<tr>
<td>4. 2 3 6</td>
<td>4. b a b</td>
</tr>
<tr>
<td>5. a r e</td>
<td>5. p r i</td>
</tr>
</tbody>
</table>

- The top 5 choices for two of the \( \binom{n}{m} = 56 \) challenges
- Dictionary is RockYou (8-char alphanumeric) with frequencies
- 5.3m total, top 5 words in ranked dictionary covers 3.02%
- Top 5 full words: password, iloveyou, princess, 12345678, babygirl
Example projection dictionary attack

- This shows the coverage of guesses for increasing $\beta$
- Each line is a different challenge, bold is average
- Success rate for $\beta=10$ is 5.5% versus 3.9% without projection
Recording Attacks
Mode of attack for recording

- online, $\beta$ attempts per challenge, as before
- allow recording previous $k$ challenge-response pairs

**Recording methods**

1. **Pure recording**: only answer when positions known
2. **Recording+guessing**: guess remainder of positions

Combinatorics: we find equations for two different success rates for increasing $k$. They are probabilities of:

- answering the **next challenge**, or
- learning the **whole password**.
Success rates for answering next challenge

This is a plot of

\[
\sum_{j=0}^{m} s_{n}^{m}(k, j)w_{j}
\]

where \(0 \leq j \leq m\) positions are known in a challenge after \(k\) runs.

- \(s_{n}^{m}(k, j)\): fraction of challenges with \(j\) known positions
- \(w_{j}\): the \(\beta\)-success rate for a particular guessing method
Summary
### Results for typical parameters

<table>
<thead>
<tr>
<th>Attack type</th>
<th>parameters</th>
<th>PINs</th>
<th>alphanumeric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brute force</td>
<td></td>
<td>6</td>
<td>0.002</td>
</tr>
<tr>
<td>Letter position</td>
<td>RockYou</td>
<td>17.2</td>
<td>0.3</td>
</tr>
<tr>
<td>Dictionary</td>
<td>RockYou</td>
<td>15.3</td>
<td>3.9</td>
</tr>
<tr>
<td>Proj. dictionary</td>
<td>RockYou</td>
<td>30.6</td>
<td>5.5</td>
</tr>
<tr>
<td>Recording</td>
<td>$k=1$ ($k=4$)</td>
<td>6.7 (63.1)</td>
<td>1.8 (59.0)</td>
</tr>
<tr>
<td>Recording + BF Guess</td>
<td>$k=1$ ($k=4$)</td>
<td>41.1 (83.8)</td>
<td>9.6 (69.1)</td>
</tr>
<tr>
<td>Recording + Best Dict</td>
<td>$k=1$ ($k=4$)</td>
<td>60.2 (90.4)</td>
<td>25.2 (81.2)</td>
</tr>
</tbody>
</table>
Summary

- survey of partial password implementations
- model of partial password authentication scheme
- several attack methods, guessing and recording
- theoretical success rates measured analytically (pure recording) and empirically (using a dictionary)

Future/ongoing work:
- Better attacks (dependent case)
- Unseen challenge (Goring et al, 2007)
- Failure modes, challenge schedule and format
- General study of multi-stage authentication
- Discuss more with banks...