Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology

S M Taiabul Haque (University of Central Missouri)
Mahdi Nasrullah Al-Ameen (Clemson University)
Matthew Wright (Rochester Institute of Technology)
Shannon Scielzo (UT Southwestern Medical Center)

USEC 2017
System-assigned Random Password

Password: patriots
Password: patriots
Password: Patriots12
Password: tombrady
**System-assigned Random Password**

![Image of worst passwords of 2012]

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Change from 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>#2</td>
<td>123456</td>
<td></td>
</tr>
<tr>
<td>#3</td>
<td>12345678</td>
<td></td>
</tr>
<tr>
<td>#4</td>
<td>abc123</td>
<td></td>
</tr>
<tr>
<td>#5</td>
<td>qwerty</td>
<td></td>
</tr>
<tr>
<td>#6</td>
<td>monkey</td>
<td></td>
</tr>
<tr>
<td>#7</td>
<td>letmein</td>
<td></td>
</tr>
<tr>
<td>#8</td>
<td>dragon</td>
<td></td>
</tr>
<tr>
<td>#9</td>
<td>111111</td>
<td></td>
</tr>
<tr>
<td>#10</td>
<td>baseball</td>
<td></td>
</tr>
</tbody>
</table>

*Legend: unchanged, up, down*
System-assigned Random Password
Research Constraints

• Entropy (minimum 20 bits)

• Time ( < 3 minutes )

• Automation (no unaided user action)
Memorization Techniques
Method of Loci

The phone number to be remembered is in sequence to where each digit is associated with the landmark on the trail.

934-7589
Link/Story Method
Sample Clip (The Method of Loci)

Your Password is: PKURSG

We will show you a video clip to help you memorize this password
Sample Screenshots (The Link Method)
Development Platform/Tool

- Max3D
- Unity3D
- Adobe Photoshop CS5
- C#
Pilot Study
System Design (Registration)

• Randomly assign a password with six lowercase letters

• Generate a video based on the assigned password

• Quick adoption of the memorization techniques
Study Design

• Within-group

• 52 participants (psychology research pool)

• Control, Loci, and Link

• Follow-up study after a week
Results (Memorability)

- Loci > Control ($p < 0.01$)
- Link > Control ($p < 0.05$)
- Loci > Link ($p < 0.05$)
Results (Login Time)

• Median login time:
  - Control 5 seconds
  - Link 6 seconds
  - Loci 9 seconds

• Nominal compared to recognition-based methods
## Results (User Feedback)

<table>
<thead>
<tr>
<th>Category</th>
<th>Loci</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficacy in providing satisfactory memorability</td>
<td>Median: 4</td>
<td>Median: 3</td>
</tr>
<tr>
<td></td>
<td>Mode: 5</td>
<td>Mode: 2</td>
</tr>
<tr>
<td>Requirement of writing down the password</td>
<td>Median: 4</td>
<td>Median: 4</td>
</tr>
<tr>
<td></td>
<td>Mode: 5</td>
<td>Mode: 4</td>
</tr>
<tr>
<td>Time spent for learning was worth it</td>
<td>Median: 4</td>
<td>Median: 3</td>
</tr>
<tr>
<td></td>
<td>Mode: 5</td>
<td>Mode: 2</td>
</tr>
</tbody>
</table>

5-point scale, higher score indicates a positive result
Cryptographically-strong Passwords

• < 20 bits (PIN-level)

• 20 – 60 bits (password-level)

• > 60 bits (crypto-level)
Spaced Repetition

![Graph showing memory retention over time. Immediate recall at 100%, decreasing to 20% after 9 hours.]

- Immediate recall: 100%
- 20 minutes: 60%
- 1 hour: 40%
- 9 hours: Approximately 20%
Spaced Repetition

• Log into a website up to 90 times across 15 days

• 82% recall success rate

• Is there an alternative, can we do it in just one session?
Method of Loci for Cryptographically-strong Secrets

- Extend from six to twelve loci
- Include a virtual office model
- A reception room, a copier room, a file cabinet room, a cubicle room, a recreation room, and a conference room
Study 2

Assigned a random password with twelve lowercase letters

Showed the video clip

Showed the portion again

Forgot?

Missed Order?

Asked to write the name of the twelve objects sequentially

Final revision
Study 2 (Session 1)

- 26 participants
- 10-dollar Subway gift card
- Returned after a week for follow-up

Mean registration time 12 minutes 16 seconds
Study 2 (Session 2)

- Three attempts to recall the password
- Hint showed if failed after three attempts
- Showed the twelve loci without the objects
Results

• 15 out of 26 (58%) without the hint

• 21 out of 26 (81%) with the hint

• Median login time 28 seconds without the hint and 171 seconds with the hint
Conclusion

• First study to apply the method of loci to help users memorize system-assigned passwords

• Sufficient password-level strength, easy-to-follow video clip, reasonable training duration, no unaided user action, no login overhead (Study 1)

• Method of loci can be leveraged to help users memorize a cryptographically-strong secret in just one session (Study 2)