Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords

Jeremiah Blocki
Saranga Komanduri
Lorrie Cranor
Anupam Datta

NDSS 2015
Motivation
Usability Problem

I changed all my passwords to "incorrect."

So whenever I forget, it will tell me "Your password is incorrect."

WeirdNutDaily.com
Security Problem

• Password breaches at major companies have affected millions of users.
Previous Work: Shared Cues

Public Cue

Private

Action: kicking

Object: penguin

PWD

Kic + Pen + ... + Pir

PWD

Kic + Lio + ... + Kis

Source: Naturally Rehearsing Passwords [BBD13]
Previous Work: Shared Cues

Combinatorial Design: Each pair of accounts has at most $\gamma$ secret stories in common.

Source: Naturally Rehearsing Passwords [BBD13]
## Previous Work: Shared Cues

<table>
<thead>
<tr>
<th>PAO Stories</th>
<th>#Passwords</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>
### Previous Work: Shared Cues

<table>
<thead>
<tr>
<th>PAO Stories</th>
<th>#Passwords</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

Adversary with one password is unlikely to crack any other password.
<table>
<thead>
<tr>
<th>PAO Stories</th>
<th>#Passwords</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>75+</td>
<td><img src="image" alt="Devil" /></td>
</tr>
<tr>
<td>15</td>
<td>75+</td>
<td><img src="image" alt="Devil" /> <img src="image" alt="Devil" /></td>
</tr>
<tr>
<td>43</td>
<td>75+</td>
<td><img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /> <img src="image" alt="Devil" /></td>
</tr>
</tbody>
</table>
User Study Goals

• Spaced Repetition
  – Can users recall multiple PAO stories by following spaced repetition schedules?
  – Which schedules work best?

• Mnemonic Advantage
  – Does the PAO mnemonic technique improve recall?

• Interference Effect
Outline

• Motivation
• Study Protocol
  – Recruitment and Incentives
  – Memorization Phase
  – Rehearsal Phase
  – Conditions
• Results
• Discussion
• Future Directions
Recruitment

578 participants completed initial memorization phase
User Study Protocol

• Memorization Phase (5 minutes):
  – Participants asked to memorize four randomly selected person-action object stories.

• Rehearsal Phase (120+ days):
  – Participants periodically asked to return and rehearse their stories (following rehearsal schedule)
Memorization Phase

Please select a person from the drop-down list to go with the scene above. Once you choose a person for this scene, you cannot change your selection. Press the Continue button when finished.

Continue

Click the image to choose a different picture
Memorization Phase

Your words are: bribing roach.
Imagine the person you have selected performing this action in the scene above. Type in a short story involving the person, action, and object. Make sure your words appear in your story, in the correct order. Select representative images for the actions and objects above by clicking on the placeholder images beneath the words.

Type your words twice in the boxes below.

<table>
<thead>
<tr>
<th>Action</th>
<th>Object</th>
</tr>
</thead>
</table>

Continue
Rehearsal

Please enter the pair of words that you were assigned.
Rehearsal Schedules

Example 1: **12hrX1.5**

First Rehearsal \((t_1)\): 12 hours
Example 1: 12hrX1.5

First Rehearsal ($t_1$): 12 hours

\[ t_{i+1} - t_i = 12hr \times (1.5)^i \]
Rehearsal Schedules

Example 1: 12hrX1.5

Final Rehearsal ($t_{10}$): 157 days

$t_{i+1} - t_i = 12hr \times (1.5)^i$

Day: 0 16 32 48 64 80 96 112 128 144 160
Rehearsal Schedules

Example 2: **24hrX2**

First Rehearsal ($t_1$): 24 hours

$t_{i+1} - t_i = 24hr \times (2)^i$

Day: 0 16 32 48 64 80 96 112 128 144 160
Rehearsal Schedules

Example 2: 24hrX2

Final Rehearsal ($t_7$): 127 days

$t_{i+1} - t_i = 24 \text{hr} \times (2)^i$

Day: 0  16  32  48  64  80  96  112  128  144  160
# Rehearsal Schedules

<table>
<thead>
<tr>
<th>Rehearsal# Schedule</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>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>12hrx1.5</td>
<td>.5 day</td>
<td>1.75</td>
<td>4.2</td>
<td>8.2</td>
<td>14.7</td>
<td>24.7</td>
<td>40.7</td>
<td>64.7</td>
<td>101.7</td>
<td>157.7</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>24hrX2</td>
<td>1 day</td>
<td>3</td>
<td>7</td>
<td>15</td>
<td>31</td>
<td>63</td>
<td>127</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>24hrX2+2Start</td>
<td>.1 day</td>
<td>.6</td>
<td>1.6</td>
<td>3.6</td>
<td>7.6</td>
<td>15.6</td>
<td>31.6</td>
<td>63.6</td>
<td>127.6</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>30minX2</td>
<td>.5 hr</td>
<td>1.5 hr</td>
<td>3.5 hr</td>
<td>7.5 hr</td>
<td>15.5 hr</td>
<td>1.7 day</td>
<td>3.7</td>
<td>7.7</td>
<td>15.7</td>
<td>31.7</td>
<td>63.7</td>
<td>127.7</td>
</tr>
</tbody>
</table>
Incentives

• Memorization Phase ($0.5)

• Rehearsal Phase ($0.75 each)
  – Encourage participants to return
  – Discourage Cheating
Do Not Write Down Your Words

• “…we ask that you do not write down the words that we ask you to memorize.”
Do Not Write Down Your Words

• “...we ask that you do not write down the words that we ask you to memorize.”
• “You will be paid for each completed rehearsal phase --- even if you forgot the words.”
• “Important: ...do not write down the words”
• “You will be paid for each completed rehearsal phase --- even if you forgot the words.”
Study Conditions

• Mnemonic/text

• Rehearsal Schedule

• # PAO Stories
  – One, Two or Four

m_12hrX1.5_4
## Study Conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>m_24hrX2+2Start_1</td>
<td>1 PAO Story</td>
</tr>
<tr>
<td>m_24hrX2+2Start_2</td>
<td>2 PAO Stories</td>
</tr>
<tr>
<td>m_24hrX2+2Start_4</td>
<td>4 PAO Stories</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>t_24hrX2+2Start_4</td>
<td>Text condition/No Cues</td>
</tr>
<tr>
<td>m_24hrX2+2Start_4</td>
<td>Mnemonic Condition</td>
</tr>
<tr>
<td>Condition</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>m_24hrX2_4</td>
<td>24 hour base</td>
</tr>
<tr>
<td>m_24hrX2+2Start_4</td>
<td>Two Extra Rehearsals on Day 1</td>
</tr>
<tr>
<td>m_30minX2_4</td>
<td>30 min base</td>
</tr>
<tr>
<td>m_12hrX1.5_4</td>
<td>Growth Rate: 1.5x</td>
</tr>
</tbody>
</table>
Survey: Dropped Participants

Which of the following reasons did participants give for being unable to return to the study?

- Would not be able to remember the words
- Generally do not participate in follow-up studies
- Did not see the e-mail until it was too late
- I was too busy
- No longer wished to participate

(Participant did not respond to survey)

No participant self-reported that they didn’t return because the stories were too difficult to memorize.
Survey: Dropped Participants

Which of the following reasons best describes why you were unable to return to take the follow up test?

- (Participant did not respond to survey)
- Generally do not participate in follow up studies
- Would not be able to remember the words
- Did not see the e-mail until it was too late
- I was too busy
- No longer wished to participate
Outline

• Motivation
• Study Protocol
• Results
• Discussion
• Future Directions
Rehearsal Schedules

Survived(i)/Returned(i)
Rehearsal Schedules

Survived(i)/Returned(i)

Exp(\(\beta\)) = 0.42 *

* Statistically Significant (p=0.05)

Participants twice as likely to fail at any given point in time
Text vs Mnemonic

Survived(i)/Returned(i)

m_24hrX2+2Start

0.00 0.25 0.50 0.75 1.00

0 50 100 150

Survived(i)/Returned(i)

t_24hrX2+2Start

0.00 0.25 0.50 0.75 1.00
Text vs Mnemonic

Advantage is statistically significant
Text vs Mnemonic

Advantage is not statistically significant

Survived(i)/Returned(i)
Interference

Survived(i)/Returned(i)

Interference Effect was Statistically Significant
Outline

• Motivation
• Study Protocol
• Results
• Discussion & Future Directions
  – Password Expiration Policies
  – Password Strengthening
  – Mitigating Interference
Our Take: Password Expiration Policies

High Effort Region

Low Effort Region

Day: 0 16 32 48 64 80 96 112 128 144 160
We believe our study calls into question the merit of continuing the practice of password expiration.

Yinqian Zhang
University of North Carolina at Chapel Hill
Chapel Hill, NC
yinqian@cs.unc.edu

Fabian Monrose
University of North Carolina at Chapel Hill
Chapel Hill, NC
fabian@cs.unc.edu

Michael K. Reiter
University of North Carolina at Chapel Hill
Chapel Hill, NC
reiter@cs.unc.edu

ABSTRACT

This paper presents the first large-scale study of the success of password expiration in meeting its intended purpose, namely revoking access to an account by an attacker who has captured the account’s password. Using a dataset of over 7700 accounts, we assess the extent to which passwords that users choose to replace expired ones pose an obstacle to the attacker’s continued access. We develop a framework by which an attacker can search for a user’s new password from an old one, and design an efficient algorithm to build an approximately optimal search strategy. We then use this strategy to measure the difficulty of breaking newly chosen passwords from old ones. We believe our study calls into question the merit of continuing the practice of password expiration.

an attacker wants to do all of the damage that he’s going to do right now. It does offer a benefit when the attacker intends to continue accessing a system for an extended period of time. [2]

At this level of specificity, such an argument is unquestionably sound. However, the process of reducing such intuition to a reasonable password expiration policy would ideally be grounded in measurements of what “additional steps” the policy hoists on an attacker, so as to be certain that these “additional steps” are an impediment to his continued access. Unfortunately, even to this day, the security community has yet to provide any such measurements.

In this paper we provide the first analysis of which we are aware of the effectiveness of expiring passwords. Using a dataset of pass-
We believe our study calls into question the merit of continuing the practice of password expiration.
Password Strengthening

• Towards reliable storage of 56-bit secrets in human memory [BS14]
Related Work

Day: 0

Day: 0   16   32   48   64   80   96   112   128   144   160
Password Strengthening Mechanism

jblocki, Abcd1234

Bouncing, Smore
Password Strengthening Mechanism

Welcome!

Abcd1234 + ?

Bouncing, Smore

jblocki
Password Strengthening Mechanism

Welcome!
Once we can be confident that the user will remember the story we add it to the password.
Future Directions

• Understand the Cause(s) of Interference
  – User Fatigue?
  – Mixing up stories?

• Mitigating Interference
  – Staggered Memorization Schedule?
  – Gracefully Expanding Combinatorial Designs
Future Directions

• Spaced Repetition with other mnemonics
  – Graphical Secrets
Thanks for Listening
Conclusion

Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords

<table>
<thead>
<tr>
<th>Pwd</th>
<th>Kic + Pen + ... + Pir</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pwd</th>
<th>Kic + Lio + ... + Kis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|     |                        |
|     |                        |
|     |                        |
|     |                        |
Related Work

• Password Management Software

![LastPass](image)

![Stanford PwdHash](image)
Related Work

**Goal:** Minimize Trust Assumptions about User’s Computational Devices
Related Work

• Alternatives to Passwords
Related Work

Quest to Replace Passwords [BHOS2012]