Password Research at STEEL Group

Jelena Mirkovic
Information Sciences Institute (ISI)
Marina Del Rey
Passwords: Necessary and Bad

- Everyone uses passwords
- Many problems:
  - Memorable passwords are easily cracked
  - Secure passwords hard to remember
  - Similar/same passwords are used for multiple accounts
Security Qs And Passphrases

Security Questions
• Not generally applicable
• Memorable but easily guessed
• People provide fake answers

Passphrases
• Longer than passwords
• Predictable
Three Select Projects

• *Life-Experience Passwords*: How to use existing memories to build a new type of passwords

• *MNPass*: How to use mnemonics to improve passphrases

• *SemTrac*: How people reuse passwords
Life-Experience Passwords (LEPs)

with Simon Woo (USC CS), Elsi Kaiser (USC Psycholinguistics), Ron Artstein (ICT NLP)
Motivation of LEPs

• Users create passwords based on facts they remember about past events from their life (no burden on memory)

• Relying on existing events makes LEPs
  – Memorable (no new memories)
  – Unique (each person is different)
  – Less reused (abundance of memories to choose from)
Example

Title: My wedding
Which city did you get married in: Paris
Who did your makeup: Samantha Cox
Who brought chocolate cake: Jillian Grey
What did your mom bring as a gift: red scarf
What kind of ring you got: orange diamond
How LEPs work?

**CREATION**
- User input
- User title
- Processing
- Questions
- Answers
- Facts
- Hash(es)
- Store

**AUTHENTICATION**
- User answers
- Title
- Questions
- Hash(es)
- Match?
  - Yes: Authentication success
  - No: Authentication failure
LEP Design

• **Topics:** engagement, wedding, birth, death, accident, graduation, party, trip, learning a skill or language, person, place

• **Useful facts:** strong, stable and immutable
  – People, locations, time, objects, activities
  – Elicitation specificity matters
  – Need relaxed matching

• **Sensitive facts:** 3% of users in our study, can be minimized through better elicitation
**Title:** Trip to France

**How many memorable cities did you visit?** 2

**List two memorable cities you visited?** Paris, Nice

**When did you travel?** 2015

**How many people traveled with you?** 1

**List the first and last name of the person that traveled with you?** Nick Casey

**List two cities you visited**

- Paris
- Nice

**List a location related to "best art"**

- Paris

**List a location related to "wonderful weather"**

- Nice
User Studies

• **Performance:**
  – Study strength, recall, reuse
  – Online study, 93 Mturks
  – Asked to create 10 LEPs and 10 passwords and return to authenticate, 3 attempts

• **Friend:**
  – Study if friends can guess LEPs
  – Lab study, 100 pairs of USC students
  – Asked to create 3 LEPs and a friend can guess using personal knowledge, social networks, search engines, 3 attempts
### Strength

<table>
<thead>
<tr>
<th>Measure</th>
<th>LEP Guided</th>
<th>LEP Semi-G</th>
<th>Pass</th>
<th>SQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. Absolute Strength</td>
<td>161 bit</td>
<td>132 bit</td>
<td>53 bit</td>
<td>&lt; 53bit</td>
</tr>
<tr>
<td>Avg. Real Strength (statistical guessing)</td>
<td>99 bit</td>
<td>82 bit</td>
<td>&lt; 53 bit</td>
<td>&lt;&lt; 53bit</td>
</tr>
</tbody>
</table>

LEPs are 29-46 bits stronger than an ideal, randomized, 8-character password.
## Short-Term Recall

<table>
<thead>
<tr>
<th>Recall</th>
<th># of facts</th>
<th>LEP Guided</th>
<th>LEP Semi-G</th>
<th>Pass</th>
<th>SQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 week</td>
<td>All-fact</td>
<td>31.6%</td>
<td>45.7%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Five-fact</td>
<td>47.7%</td>
<td>45.7%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Four-fact</strong></td>
<td><strong>70%</strong></td>
<td><strong>73%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Three-fact</td>
<td>82.1%</td>
<td>89.2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>One OP/SQ</td>
<td>-</td>
<td>-</td>
<td>26%</td>
<td>32.1%-83.9%</td>
</tr>
</tbody>
</table>

LEPs are 2-3 times more memorable than passwords.
Long-Term Recall

<table>
<thead>
<tr>
<th>Recall</th>
<th># of facts</th>
<th>LEP Guided</th>
<th>LEP Semi-G</th>
<th>Pass</th>
<th>SQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-6 mo</td>
<td>All-fact</td>
<td>16.5%</td>
<td>32.3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Five-fact</td>
<td>33.9%</td>
<td>32.3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Four-fact</strong></td>
<td><strong>53%</strong></td>
<td><strong>54%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Three-fact</td>
<td>66.5%</td>
<td>73.6%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>One OP/SQ</td>
<td>-</td>
<td>-</td>
<td>9%</td>
<td>6.4%-79.2%</td>
</tr>
</tbody>
</table>

LEPs are 6 times more memorable than passwords
# Reuse

<table>
<thead>
<tr>
<th>Measure</th>
<th>Guided</th>
<th>Semi Guided</th>
<th>OP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. Identical</td>
<td>3.1%</td>
<td>2.7%</td>
<td>5.7%</td>
</tr>
<tr>
<td>Avg. Similar</td>
<td>15.4%</td>
<td>4.6%</td>
<td>31.6%</td>
</tr>
</tbody>
</table>

LEPs are reused half as often as passwords
# Friend Guessing

<table>
<thead>
<tr>
<th>Guess</th>
<th>Guided</th>
<th>Semi-Guided</th>
<th>SQs</th>
</tr>
</thead>
<tbody>
<tr>
<td>All-fact</td>
<td>3.5%</td>
<td>0%</td>
<td>-</td>
</tr>
<tr>
<td>Five-fact</td>
<td>3.5%</td>
<td>0%</td>
<td>-</td>
</tr>
<tr>
<td><strong>Four-fact</strong></td>
<td><strong>3.5%</strong></td>
<td><strong>0%</strong></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td>Three-fact</td>
<td>7%</td>
<td>5.3%</td>
<td>-</td>
</tr>
<tr>
<td><strong>Security Question</strong></td>
<td>-</td>
<td>-</td>
<td><strong>17-25%</strong></td>
</tr>
</tbody>
</table>
Using Mnemonics to Improve Passphrases

with Simon Woo (USC CS)
Mnemonic Passphrase (MNPass)

• Passphrase: sentence or collection of words
  – Longer than password ➔ more secure
  – Different passphrases hard to recall
  – Grammar/popular phrases lower security

• Mnemonic: first letters of each passphrase word
  – Use at authentication: improve memorability (hint-mnemonic)
  – Use at creation: improve strength (guide-mnemonic)
MNPass Examples

Your passphrase contains words starting with letters MLAAO

Username: 
Passphrase: 

Your passphrase must contain words starting with the displayed letters

Username: 
Passphrase: A B A L O

hint-mnemonic

guide-mnemonic
Passphrase Models

- **UPass**: all user-chosen words
- **UPassHint**: UPass + hint-mnemonic
- **MNPass(0)**: all user-chosen words using guide-mnemonic + hint+mnemonic
- **MNPass(0)-Long**: MNPass(0) + 2-3 more words
- **MNPass(1)**: MNPass(0) with one system-chosen word
- **SysPass**: all system-chosen words
- **SysPassHint**: SysPass + hint-mnemonic
User Study

- Study strength, recall
- Online study, 393 Mturks, 44-66 per model
- Participants assigned randomly into passphrase model, create one passphrase each 5 word long
- Measure recall at 3 and 7 days after creation
## Improve Recall

<table>
<thead>
<tr>
<th>Model</th>
<th>exact match (%)</th>
<th>3 day</th>
<th>7 day</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>w/o hint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upass</td>
<td>52.3</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>SysPass</td>
<td>20.7</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td><strong>w/ hint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPassHint</td>
<td>71.4</td>
<td>69.6</td>
<td></td>
</tr>
<tr>
<td>SysPassHint</td>
<td>26.8</td>
<td>18.9</td>
<td></td>
</tr>
<tr>
<td>MNPass(0)</td>
<td>69.7</td>
<td>66.7</td>
<td></td>
</tr>
<tr>
<td>MNPass(1)</td>
<td>69.3</td>
<td>67.7</td>
<td></td>
</tr>
<tr>
<td>MNPass(0)-Long</td>
<td>66.7</td>
<td>62.8</td>
<td></td>
</tr>
</tbody>
</table>
Good Strength

- Language model (LM) attacker and convert prob. of passphrases into bit-strength entropy

<table>
<thead>
<tr>
<th>Model</th>
<th>w/o hint</th>
<th>w hint</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPass/UPassHint</td>
<td>61.9</td>
<td>49.3</td>
</tr>
<tr>
<td>MNPass(0)</td>
<td>67.5</td>
<td>44.5</td>
</tr>
<tr>
<td>MNPass(1)</td>
<td>75.8</td>
<td>60.2</td>
</tr>
<tr>
<td>MNPass(0)-Long</td>
<td>84.6</td>
<td>60.3</td>
</tr>
<tr>
<td>SysPass/SysPassHint</td>
<td>84.4</td>
<td>63.5</td>
</tr>
</tbody>
</table>
Low Guessability

- Collected 280,550 famous phrases from web
- Compute ordered overlapped words between famous phrases and passphrases

<table>
<thead>
<tr>
<th>Model</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3+</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPass/UPassHint</td>
<td>0</td>
<td>8.4</td>
<td>39.5</td>
<td>52</td>
</tr>
<tr>
<td>MNPass(0)</td>
<td>0</td>
<td>34.8</td>
<td>60.6</td>
<td>4.5</td>
</tr>
<tr>
<td>MNPass(1)</td>
<td>8</td>
<td>50</td>
<td>38.7</td>
<td>3.2</td>
</tr>
<tr>
<td>MNPass(0)-Long</td>
<td>5.9</td>
<td>17.6</td>
<td>58.8</td>
<td>17.6</td>
</tr>
<tr>
<td>SysPass/SysPassHint</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Summary

Recall

- Hint-mnemonics improve recall by 30–36% after three days and 51–74% after seven days.
- Hints aid recall of important facts.
- MNPass recall is comparable to UPass recall

Strength

- Mnemonic-guided comparable to system-chosen approach
Understanding Password Reuse

with Simon Woo (USC CS), Ameya Hanamsagar (USC CS), Chris Kanich (UIC CS)
Password Reuse

- People remember only 5 or 6 passwords over 30 online accounts[1]
- Cognitive burden (security fatigue) on memorizing multiple passwords
- Many passwords have similar patterns, which can result in password re-use attack

Measure Password Reset Request

From: chase.com
Message: Please reset your password

From: facebook.com
Message: Please change your password

OAuth
Detect Similar Passwords

Chrome Extension: Semantically Transform Passwords

Password: John@4r
Password: !2jane

John@4r → Bob#1a
!2jane → ?8mary

Preserve user privacy and extract semantics
User Study (on-going)

- 50 participants
- Let us scan their Gmail account and then attempt to log into 12 sites
- Divide accounts into important (financial/email) and non-important
- Store semantically transformed passwords and ask users about
  - Risk perception
  - Understanding of attacks and reuse
Preliminary Findings

- 83% share passwords between imp/non-imp sites
- Password strength low
  - Users create longer passwords for important sites but they are not stronger
- 90% do not know how automated crackers work
  - Think that they need access to personal information
- Security fatigue leads to reuse – don’t care attitude
- Users reveal their important site passwords when failing to log into a non-important site
Conclusion

• Password memorability very important to users
• Users understand security requirements but cannot follow them
• LEPs and mnemonics reasonable solutions to improve memorability and strength of passwords and passphrases
• Need more solutions
Thank You !