Human Computable Protocols: Password-based Authentication

Anupam Datta

With Jeremiah Blocki and Manuel Blum

Carnegie Mellon University
# Memory Experiment 1

<table>
<thead>
<tr>
<th>Person</th>
<th>Bill Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Tickling</td>
</tr>
<tr>
<td>Object</td>
<td>Peach</td>
</tr>
</tbody>
</table>
Memory Experiment 2

<table>
<thead>
<tr>
<th>Person</th>
<th>Michelle Obama</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Bouncing</td>
</tr>
<tr>
<td>Object</td>
<td>Smore</td>
</tr>
</tbody>
</table>
Password Management

Competing Goals:

Security → Usability
Security Problem

• Password breaches at major companies have affected millions of users.
Traditional Security Advice

- Use numbers and letters
- Use special symbols
- Don’t Reuse Passwords
- Not too short
- Don’t use words/names
- Don’t Write it Down
- Use mix of lower/upper case letters
- Change your passwords every 90 days
Usability Problem

I changed all my passwords to "incorrect".

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

WeirdNutDaily.com
Fundamental Question

- How can we evaluate password management strategies?
  - Quantify Usability
  - Quantify Security
Outline

• Introduction
  – Motivation
  – Our Approach
  – Related Work
• Usability and Security Models
• Shared Cues
• Human Computable Passwords
• Conclusion and Future Vision
Traditional Approach

Propose New Password Management Scheme

User Study: Evaluate New Password Management Scheme
Our Thesis

User models and security models can guide the development of human authentication schemes with analyzable usability and security properties.
Our Approach: User Models

User Model
Capabilities + Behavior

Example Capability: Users can remember a random secret with enough rehearsal.

Example Behavior: How often a user visits each website on average.
Our Approach: User Models

User Model
Capabilities + Behavior

Develop + Analyze
User Model
Empirical Validation

Fast: Evaluation does not require expensive user studies
can be used to analyze broad class of password management schemes
### Research Results

#### Defense Adopted by

<table>
<thead>
<tr>
<th>Result</th>
<th>User</th>
<th>Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Computable Passwords [BBDV---]</td>
<td></td>
<td>GOTCHA Password Hackers [BBD2013]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cost Asymmetric Secure Hash [BBD---]</td>
</tr>
</tbody>
</table>

- **Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords [BKCD2015]**

- **Develop + Analyze**
- **User Model**
- **Empirical Validation**

**Venues:** NDSS, ASIACRYPT, EC, AISEC
Preview of Results

- Human Computable Passwords
- Independent Strong Passwords
- Shared Cues
- Reuse Weak Password

User Effort vs. Security
Outline

- **Introduction**
  - Motivation
  - Our Approach
  - Related Work

- Usability and Security Models

- Shared Cues

- Human Computable Passwords

- Conclusion and Future Vision
Related Work

Challenge: Multiple Passwords

- Graphical Passwords
  - Passfaces
  - Cued Click Points
  - Windows 8

...
Related Work

**Goal:** Quantify Security for Multiple Passwords
Related Work

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

Quest to Replace Passwords [BHOS2012]
Outline

• Introduction

• **Usability and Security Models**
  – Example Password Management Schemes
  – Usability Model
  – Security Model

• Shared Cues

• Human Computable Passwords

• Conclusion and Future Vision
Scheme 1: Reuse Strong Password

- Pick four random words $w_1, w_2, w_3, w_4$

<table>
<thead>
<tr>
<th>Account</th>
<th>Amazon</th>
<th>Ebay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>$w_1 w_2 w_3 w_4$</td>
<td>$w_1 w_2 w_3 w_4$</td>
</tr>
</tbody>
</table>
Scheme 2: Strong Random Independent

Four Independent Random Words per Account

<table>
<thead>
<tr>
<th>Account</th>
<th>Amazon</th>
<th>Ebay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>$w_1 w_2 w_3 w_4$</td>
<td>$x_1 x_2 x_3 x_4$</td>
</tr>
</tbody>
</table>
Outline

• Introduction
• **Usability and Security Models**
  – Example Password Management Schemes
  – **Usability Model**
  – Security Model
• Shared Cues
• Human Computable Passwords
• Conclusion and Future Vision
First Attempt: Chunking

- Memorize: nbccbsabc
- Memorize: tkqizrlwp
- 3 Chunks vs. 9 Chunks!

Usability Goal: Minimize Number of Chunks in Passwords

Source: The magical number seven, plus or minus two [Miller, 56]
Human Memory: Vast, but Lossy

- Rehearse or Forget!
  - How much work?
- Quantify Usability
  - Rehearsal Assumption
Memory Capability

Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval \([s^i, s^{i+1}]\).

Source: *Optimization of Repetition Spacing in the Practice of Learning* [WG, 94]
Memory Capability

Source: Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords [BKCD15]
Natural Rehearsal

Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval \([s^i, s^{i+1}]\).

**X_t**: extra rehearsals to maintain *all* passwords for *t* days.

Source: *Optimization of Repetition Spacing in the Practice of Learning* [WG, 94]
Extra Rehearsals

\( X_t \): extra rehearsals to maintain \( all \) passwords for \( t \) days.

<table>
<thead>
<tr>
<th></th>
<th>Reuse Password</th>
<th>Independent Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_0 )</td>
<td>Minimize ( X_t )</td>
<td>2</td>
</tr>
</tbody>
</table>
### Usability Results

<table>
<thead>
<tr>
<th></th>
<th>Reuse Strong</th>
<th>Strong Random Independent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>0.002</td>
<td>2,938</td>
</tr>
<tr>
<td>Typical</td>
<td>0.023</td>
<td>2,974</td>
</tr>
<tr>
<td>Occasional</td>
<td>0.109</td>
<td>3,135</td>
</tr>
<tr>
<td>Infrequent</td>
<td>3.239</td>
<td>4,024</td>
</tr>
</tbody>
</table>

$E[X_{\infty}]$: Extra Rehearsals to maintain *all* passwords over lifetime. $m = 75$ accounts, $s=1.5$