Password Coping Mechanisms
Austin Klasa, Dr. Melissa Dark

Motivation
- Passwords are the most common means of authenticating users
- The number of passwords a user must select and manage is increasing
- Password policies are complex

Background Research
- Formulate Taxonomy
- Write and Test Analysis Program
- Run Analysis Program on Data
- Analyze Results

Password Coping Mechanisms (PCM)
- Any password selection and management behavior used to cope with the large number of passwords a user must remember for multiple accounts, and the complexity of password policies
- Organized by the password coping mechanism taxonomy (below)

Background Research
- Formulate Taxonomy
- Write and Test Analysis Program
- Run Analysis Program on Data
- Analyze Results

Password Coping Mechanisms (PCM)
- Any password selection and management behavior used to cope with the large number of passwords a user must remember for multiple accounts, and the complexity of password policies
- Organized by the password coping mechanism taxonomy (below)

Citation: Curnett, B. (2015). Password Strength Analysis: User Coping Mechanisms in Password Selection. Purdue University.

Research Questions
1. What percentage of users engage in each password coping mechanism subcategory shown in the taxonomy? Completed, see table.
2. Which password coping mechanism subcategories are frequently combined by users to create hybrid password coping mechanisms?
3. Which password coping mechanism subcategories are most frequently used by certain demographics?

Methodology
- Data Set:
  - Originally created by Curnett (2015)
  - Utilized Amazon Mechanical Turk
  - Contains multiple iterations of passwords and demographic information for 1032 users
- A subset of PCMs from the taxonomy can be analyzed with a password data set
- A program analyzes the passwords from each user to determine if they have used any PCMs

Future Work
- Code refactoring and documentation
- Statistical analysis:
  - Differences between password policies
  - User level granularity
  - Hybrid PCMs
  - PCMs by demographic

PCM Prevalence
- Results for research question 1
- Shows the percent of users that engage in a PCM
- * only includes users that have the character in their password

<table>
<thead>
<tr>
<th>PCM</th>
<th>True (%)</th>
<th>False (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Changing</td>
<td>11.1</td>
<td>88.9</td>
</tr>
<tr>
<td>Different Iterations</td>
<td>21.8</td>
<td>78.2</td>
</tr>
<tr>
<td>Sequence</td>
<td>52.6</td>
<td>47.4</td>
</tr>
<tr>
<td>Word</td>
<td>55.6</td>
<td>44.4</td>
</tr>
<tr>
<td>Common Password</td>
<td>13.1</td>
<td>86.9</td>
</tr>
<tr>
<td>Context Linking</td>
<td>2.0</td>
<td>98.0</td>
</tr>
<tr>
<td>Non-Distinct</td>
<td>20.8</td>
<td>79.2</td>
</tr>
<tr>
<td>Reverse</td>
<td>46.5</td>
<td>53.5</td>
</tr>
<tr>
<td>Capital Letter*</td>
<td>92.5</td>
<td>7.5</td>
</tr>
<tr>
<td>Digit*</td>
<td>91.2</td>
<td>8.8</td>
</tr>
<tr>
<td>Special Character*</td>
<td>80.7</td>
<td>19.3</td>
</tr>
<tr>
<td>Leet</td>
<td>5.4</td>
<td>94.6</td>
</tr>
</tbody>
</table>