Rethinking Passwords


- 1985 DoD CSC *Password Management Guideline*, aka the Green Book
Vulnerabilities of Password Systems

1. A password must be initially assigned to a user when enrolled on the system.
2. A user's password must be changed periodically.
3. The system must maintain a password database.
4. Users must remember their passwords
5. Users must enter their passwords into the system at authentication time.
Other Guidelines

- Users should be able to change their passwords.
- Passwords should be machine-generated rather than user-generated.
- Certain audit reports (e.g., date and time of last login) should be provided by the system directly to the user.
- User ID is a unique symbol or character string that is used by a system to uniquely identify a user.
Other Guidelines

• Throughout the lifetime of a system, each user ID should be assigned to only one person.
• All user IDs should be revalidated periodically.
• The simplest way to recover from the compromise of a password is to change it.
• Passwords should be changed on a periodic basis.
Goal: crack probability of $10^{-6}$ after 1 year of dictionary attacks

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Search space (bits)</th>
<th>7 billion trials/second</th>
<th>10 million trials/second</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Cracked in</td>
<td>Change time</td>
</tr>
<tr>
<td>8-character, full alphanumeric</td>
<td>47.6</td>
<td>0.36 mins.</td>
<td>31.19 ms.</td>
</tr>
<tr>
<td>8-character, eye-of-newt</td>
<td>52.3</td>
<td>9.25 days</td>
<td>799.40 ms.</td>
</tr>
<tr>
<td>11-character, eye-of-newt</td>
<td>71.9</td>
<td>20,390 years</td>
<td>7 days</td>
</tr>
<tr>
<td>13-character, full alphanumeric</td>
<td>77.4</td>
<td>906,123 years</td>
<td>331 days</td>
</tr>
<tr>
<td>12 character, eye-of-newt</td>
<td>78.5</td>
<td>1,896,229 years</td>
<td>692 days</td>
</tr>
</tbody>
</table>
Other Aphorisms

- Do not use the same password on multiple services.
- Do not write your passwords down.
- Change your passwords often.