Employee Password Usability Survey

Yee-Yin Choong

Visualization and Usability Group
Information Access Division
Information Technology Laboratory
National Institute of Standards and Technology

September 10, 2015
Employee Password Management

- **Online Survey**
  - Anonymous
  - Questions on password management and computer security
  - Demographics

- **US Government Workers**
  - 4,573 Department of Commerce (DOC) employees
Demographics

• Gender

- Male: 57.5%
- Female: 39.2%
- na: 3.3%

• Education

- HS: 7.0%
- Asso: 5.3%
- BS: 34.4%
- MS: 31.7%
- PhD: 15.6%
- Prof degree: 2.7%
- na: 1.4%
Demographics

- **Age** (years)

<table>
<thead>
<tr>
<th>Age Interval</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 25</td>
<td>3.5%</td>
</tr>
<tr>
<td>26–35</td>
<td>20.5%</td>
</tr>
<tr>
<td>36–45</td>
<td>23.1%</td>
</tr>
<tr>
<td>46–55</td>
<td>29.8%</td>
</tr>
<tr>
<td>56–65</td>
<td>18.6%</td>
</tr>
<tr>
<td>&gt; 65</td>
<td>2.4%</td>
</tr>
<tr>
<td>na</td>
<td>2.0%</td>
</tr>
</tbody>
</table>

- **Service Length** (years)

<table>
<thead>
<tr>
<th>Service Length Interval</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 1</td>
<td>5.5%</td>
</tr>
<tr>
<td>1–3</td>
<td>13.4%</td>
</tr>
<tr>
<td>4–5</td>
<td>7.7%</td>
</tr>
<tr>
<td>6–10</td>
<td>15.1%</td>
</tr>
<tr>
<td>11–14</td>
<td>11.3%</td>
</tr>
<tr>
<td>15–20</td>
<td>11.5%</td>
</tr>
<tr>
<td>&gt; 20</td>
<td>35.1%</td>
</tr>
<tr>
<td>na</td>
<td>0.5%</td>
</tr>
</tbody>
</table>
Demographics

- **Job Level**
  - Non-supervisor: 62.6%
  - Supervisor: 13.8%
  - Team lead: 11.5%
  - Manager: 9.6%
  - Executive: 1.9%
  - na: 0.6%

- **Computer Experience**
  - Novice: 0.5%
  - Average: 29.0%
  - Advanced: 50.6%
  - Expert: 19.5%
  - na: 0.3%
Findings – Outline

- Password Usage
- Attitudes toward Password Policy
- Password Management Lifecycle
  - Generation
  - Maintenance
  - Authentication
Password Usage

- **Average 9 work-related passwords**
  - 5 frequently used
  - 4 occasionally used

- **Time spent on creating passwords**

<table>
<thead>
<tr>
<th>Password Types</th>
<th>Estimated Longest Time Total&lt;sup&gt;1&lt;/sup&gt; (Mean)</th>
<th>Worst Scenario - time spent annually&lt;sup&gt;2&lt;/sup&gt; (with longest time)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Hours/employee/year If on a 90-day cycle</td>
</tr>
<tr>
<td>Frequent passwords</td>
<td>98.5 min</td>
<td>6.6 h</td>
</tr>
<tr>
<td>Occasional passwords</td>
<td>86.6 min</td>
<td>5.8 h</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>12.4 h</strong></td>
<td><strong>18.6 h</strong></td>
</tr>
</tbody>
</table>

<sup>1</sup> Estimated Longest Time Total = (number of password counts) x (estimated longest time for a password)

<sup>2</sup> The calculation is based on the password changing cycle of 90 days (i.e. 4 times a year), and 60 days (i.e. 6 times a year).
Password creation takes long, why?

- The program kept rejecting my password because it was not within the guidelines [sic] even though I thought I was following them.
- That 25 minutes was actual time trying to get a system to accept a password. I was so desperate [sic] I actually started asking colleagues for suggestions!
- Longer if I manage to lock myself out in doing so, or can't remember what I just changed it to and have to get it reset all over.
- Sometimes it's taken me 20 minutes to change a password to one that meets the requirements and isn't too far off from my other ones (so I can remember it!)
- Longest time is 2 days. The password expired and a default password was set. I could not change away from the default due to a lock out feature requiring that the password not be changed more than once in two days.
- There have been several times where it took so long to create a complex enough password that I forgot the password when logging in the next time and had to have it reset.
Attitudes toward Password Policy

- Too long
- Too complex
- Changed too often
  - not at the same time!
What did they say?

- The combination of length/complexity, number of different passwords, plus frequent changes makes passwords insecure, because they must be written down.
- How do you think people remember extremely complex passwords which also require to be changed every 3 months? #Wr1T31Td0wN .. yes that's 12 chars :)
- I understand that for ““security” ” reasons it is good to change a password - but seriously are we all expected to magically remember 12 different passwords, most of which are 10 characters [sic] long, and can't look like a word (I agree with the reason for the complexity - it just hard on the user).
- I make a list of the password requirements for all accounts and make one that fits all of them.
- Security has become so complex, it's interfering with being able to do a job efficiently.
- It is hard enough to come up with a 12 or so string of unique characters every three months, let alone remember 10 individual ones.
- Security has become so complex, it's interfering with being able to do a job efficiently.
Organizational Password Policy

- Protect data integrity and system security
- Control employees’ access
- Dictate employees’ password management
  - Password composition requirements
  - Password expiration
  - Reuse and history
  - Storage requirements
Employee Attitudes

• Attitudes (Fishbein & Ajzen, 1975)
  “Learned, relatively enduring dispositions to respond in consistently favorable or unfavorable ways to certain people, groups, ideas, or situations.”

• Positive employee attitudes
  • combat negative reactions to organization-wide changes or policy viewed as unfavorable
Divergent Views

Attitudes – Password Length

- Too long: 57.2%
- About right: 36.2%
- Too short: 0.9%
- Neutral: 5.7%

Attitudes – Password Complexity

- Too complex: 51.0%
- About right: 44.4%
- Too simple: 0.6%
- Neutral: 4.0%

Employee Password Management Lifecycle
Human Information Processor

Attention
Limited Resource

Working Memory

Long Term Memory

Individual Factors
- Attitudes
- Motivations
- Emotions

User Password Management Lifecycle

**Generation**
- Problem solving
- Creative thinking
- Decision making
- Limited processing capacities
  - attentions
  - interferences

**Maintenance**
- Decision making
- Memorizing
  - rehearsal
- Storing
  - storage decisions
- Organizing
- Muscle memory
  - typing

**Authentication**
- Recalling
  - retrieval cues from memory or storage
- Forgetting
  - memory decay
  - interferences
- Entering password
  - attentions
  - motor skills
  - muscle memory
  - hand-eye coordination

Change password (e.g. forgotten, expiration, compromise, synchronizing with other passwords)
Password Generation Considerations

* All comparisons are statistically significant ($p < 0.05$).
Password Generation Strategies

- **Minor change**
  - Length – About right: 61.1%
  - Length – Burdensome: 68.3%
  - Complexity – About right: 58.8%
  - Complexity – Burdensome: 71.5%

- **Existing pwd**
  - Length – About right: 36.2%
  - Length – Burdensome: 45.8%
  - Complexity – About right: 35.2%
  - Complexity – Burdensome: 48.2%

- **Recycle old pwd**
  - Length – About right: 29.7%
  - Length – Burdensome: 41.7%
  - Complexity – About right: 30.1%
  - Complexity – Burdensome: 42.9%

* All comparisons are statistically significant ($p < 0.05$).
Password Maintenance

All comparisons are statistically significant ($p < 0.05$).

### Primary password tracking methods

- **Memorize**
  - Length – About right: 69.7%
  - Complexity – About right: 64.0%
  - Length – Burdensome: 70.4%
  - Complexity – Burdensome: 62.7%

- **Paper**
  - Length – About right: 56.0%
  - Complexity – About right: 65.6%
  - Length – Burdensome: 56.8%
  - Complexity – Burdensome: 66.2%

- **File**
  - Length – About right: 26.8%
  - Complexity – About right: 30.9%
  - Length – Burdensome: 25.5%
  - Complexity – Burdensome: 32.5%

*All comparisons are statistically significant ($p < 0.05$).*
Password Tracking – paper in plain view

Attitudes toward Password Policy

- **Length Requirement**
  - About right: 15.9%
  - Burdensome: 29.1%

- **Complexity Requirement**
  - About right: 16.3%
  - Burdensome: 31.1%
Authentication Experience

* All comparisons are statistically significant ($p < 0.05$).

**Top 3 Login Problems**

- **Mistyping password**
  - Length – About right: 18.4%
  - Length – Burdensome: 33.0%
  - Complexity – About right: 18.8%
  - Complexity – Burdensome: 34.4%

- **Forgetting password**
  - Length – About right: 15.9%
  - Length – Burdensome: 29.5%
  - Complexity – About right: 13.7%
  - Complexity – Burdensome: 33.6%

- **Error message - changing password**
  - Length – About right: 16.1%
  - Length – Burdensome: 29.6%
  - Complexity – About right: 13.2%
  - Complexity – Burdensome: 34.4%

---

*Note: The graph shows the percentage of users who experience "A Lot" frustration for each of the top 3 login problems.
Thoughts on Compromised Passwords

- **Perceived Severity of Consequences on Compromised Passwords**
  - **Length**: About right (green), Burdensome (red)
  - **Complexity**: About right (green), Burdensome (red)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Length – About right</th>
<th>Length – Burdensome</th>
<th>Complexity – About right</th>
<th>Complexity – Burdensome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>13.6%</td>
<td>11.1%</td>
<td>13.7%</td>
<td>10.9%</td>
</tr>
<tr>
<td>None</td>
<td>48.3%</td>
<td>50.7%</td>
<td>33.3%</td>
<td>34.3%</td>
</tr>
<tr>
<td>Minor</td>
<td>9.3%</td>
<td>9.9%</td>
<td>10.0%</td>
<td>9.3%</td>
</tr>
<tr>
<td>Major</td>
<td>22.6%</td>
<td>22.3%</td>
<td>15.5%</td>
<td>14.5%</td>
</tr>
<tr>
<td>Depending on accounts</td>
<td>24.5%</td>
<td>24.1%</td>
<td>17.8%</td>
<td>17.5%</td>
</tr>
</tbody>
</table>

* Comparisons (*None*, *Major*, *Accounts dependent*) are statistically significant (*p < 0.05*).
What Did 4,500+ People Tell Us?

- **Staff overwhelmed** – *pushing human cognition limits*
  - different password requirements (length, complexity, expiration)
  - multiple passwords – frustration level significantly related to number of passwords

- **Statistically significant relationships**
  - Attitudes toward organizational security policies
  - Security behaviors and experiences
  - Positive attitudes
    - Compliant and strong passwords more important
    - Write-down passwords less often
    - Less frustration with login problems
    - Better understanding of password security
Promising Solution?

- Smart Cards for identification and authentication
- **Security**, multi-factors
  - Something you have – a Smart card
  - Something you know – a PIN
- **Usability**
  - Single sign-on
  - PINs easier to remember and to enter
The case of CAC (Common Access Card)

- **CAC**
  - Standard identification for Department of Defense (DoD) personnel
  - Physical access
  - Logical access

- **Online Survey**
  - Anonymous
  - Questions on CAC usage and password management
Single Sign-on Coverage

- All - 100%
  - DOD: 11.8%
  - DOC: 2.9%

- About 75%
  - DOD: 21.6%
  - DOC: 9.3%

- About 50%
  - DOD: 20.3%
  - DOC: 12.9%

- About 25%
  - DOD: 20.5%
  - DOC: 21.8%

- None - 0%
  - DOD: 25.7%
  - DOC: 53.2%
Attitudes toward Password Policy

<table>
<thead>
<tr>
<th>Length</th>
<th>DOD</th>
<th>DOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too long</td>
<td>41.4%</td>
<td>57.3%</td>
</tr>
<tr>
<td>Neutral</td>
<td>6.0%</td>
<td>5.7%</td>
</tr>
<tr>
<td>Too short</td>
<td>0.7%</td>
<td>0.9%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complexity</th>
<th>DOD</th>
<th>DOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too complex</td>
<td>32.5%</td>
<td>51.0%</td>
</tr>
<tr>
<td>Neutral</td>
<td>4.2%</td>
<td>4.0%</td>
</tr>
<tr>
<td>Too simple</td>
<td>0.5%</td>
<td>0.6%</td>
</tr>
</tbody>
</table>
Authentication Problems – Forgetting

- CAC – Forget PIN
- PWD – Forget Password

<table>
<thead>
<tr>
<th>Category</th>
<th>CAC (%)</th>
<th>PWD (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Large + Large amount</td>
<td>0.6</td>
<td>3.3</td>
</tr>
<tr>
<td>Moderate + Small amount</td>
<td>11.3</td>
<td>51.1</td>
</tr>
<tr>
<td>None</td>
<td>89.5</td>
<td>39.5</td>
</tr>
</tbody>
</table>

Frustration with Forgetting – DOD

- Statistical significance ($p < 0.05$)
  - More frustration with *Forgetting Password*
User Satisfaction with CAC

- Satisfied: 90.2%
- Dissatisfied: 1.9%
- Neutral: 7.9%
CAC benefits >> Passwords

- Fewer passwords to maintain, less forgetting
- Better attitudes
- Less frustration with authentication problems
- Time-saving
- High Satisfaction
Moving Forward

- Smartcards (e.g., PIVs, CACs) for authentication
- More research on
  - Direction of causality: *Attitudes & Behaviors*
  - Promote positive attitudes
  - Work and personal password management
  - Better organizational security policies


Yee-Yin Choong
National Institute of Standards and Technology
Gaithersburg, MD, USA
Yee-yin.choong@nist.gov