13 - Passwords

Lorrie Cranor, Blase Ur, and Rich Shay

February 24, 2015
Today’s class

• Password Creation and Use
• Threats to Passwords
• Password Policies
• Presentation of a Password Study
Password Creation and Use
Passwords

Microsoft account What's this?

attackvictim@outlook.com

Password

☐ Keep me signed in

Sign in
Password Creation

User

Service Provider

Password!1
Password Creation

User -> Service Provider

Password!1 -> Password!1
Password Creation

User → Service Provider

Password!1 → $h(\text{Password!1})$
Password Creation

User

Service Provider

Password!1 → \textcolor{blue}{h(Password!1)}

7e8d6b2fe300
Password Creation

User

Service Provider

Password!1 → $7e8d6b2fe300$

$h(\text{Password!1})$

$7e8d6b2fe300$
Authentication

User

Password!1

Service Provider

Password!1

7e8d6b2fe300
Authentication

User

Service Provider

Password!1 \( \rightarrow \) 7e8d6b2fe300

\( h(Password!1) \)

7e8d6b2fe300
Authentication

User

Service Provider

Password!1 → 7e8d6b2fe300

h(Password!1) → 7e8d6b2fe300
Password Threats
Password Threats that Ignore Strength

- Phishing
- Key logging
- Government coercion
- Writing your password down on a sticky note
Password Threats that Ignore Strength

• Phishing
• Key logging
• Government coercion
• Writing your password down on a sticky note

• Some of these can be addressed via training.
Many Threats Do Not Ignore Strength

- Password guessing is easier for some passwords than others
Online Attack

That password is incorrect. Be sure you’re using the password for your Microsoft account.

Microsoft account What’s this?

attackvictim@outlook.com

Password

☐ Keep me signed in
Online Attack

Sign-in is blocked

Sign-in with attackvictim@outlook.com is blocked for one of these reasons:

Someone entered the wrong password too many times.
Offline Attack

Service Provider

Password File

ed253d96e8954203aee83c497e8d6b2fe300535c4dd2d1a4cfdb40fc8210...

...
Offline Attack

Service Provider

- ed253d96e895
- 4203aee83c49
- 7e8d6b2fe300
- 535c4dd2d1a4
- cfdb40fc8210
- ...

Attacker

- ed253d96e895
- 4203aee83c49
- 7e8d6b2fe300
- 535c4dd2d1a4
- cfdb40fc8210
- ...

Offline Attack

2013 Examples

<table>
<thead>
<tr>
<th>Company</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>2.9 million</td>
</tr>
<tr>
<td>Evernote</td>
<td>50 million</td>
</tr>
<tr>
<td>Twitter</td>
<td>250,000</td>
</tr>
<tr>
<td>Living Social</td>
<td>50 million</td>
</tr>
</tbody>
</table>

Attacker

ed253d96e8954203aee83c497e8d6b2fe300535c4dd2d1a4cfdb40fc8210...
Offline Attack

\[ h(\text{guess}) \]

\[ 4142047431f5 \neq \]

[Attacker]

ed253d96e895
4203ae83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
...

23
Offline Attack

\[ h(\text{guess2}) \]

\[ 5ac005ee92e8 \neq \text{Attacker} \]

...
Offline Attack

\[ h(\text{Password!1}) = 7e8d6b2fe300 = \text{Attacker} \]

\[ \text{ed253d96e895} \]
\[ \text{4203aee83c49} \]
\[ \text{7e8d6b2fe300} \]
\[ \text{535c4dd2d1a4} \]
\[ \text{cfdb40fc8210} \]
\[ \text{...} \]
Password Policy

Passwords must have at least 8 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, and symbols.

New password

•••••••

8-character minimum; case sensitive

Reenter password

•••••••
Password Policies
Password Requirements

Adhere to the following password requirements, when selecting your Andrew account password:

### Must Contain
- At least 8-characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., ~!@#$%^&*(-+=).

### Cannot Contain
- Known information (i.e., first name, last name, Andrew userID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).
- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*
- A word that is found in a standard dictionary.*

**Note:** Verify that the letters within your password do not spell a word after you remove any non-alphabetical or special characters. The system checks all of the letters of the password together. [Details...]

*This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).

### Additional Policies
- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.
Password Requirements

Adhere to the following password requirements, when selecting your Andrew account password:

**Must Contain**
- At least 8 characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., ~!@#$%^&()_+=-).

**Cannot Contain**
- Known information (i.e., first name, last name, Andrew userID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).
- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*
- A word that is found in a standard dictionary.*

*Note: Verify that the letters within your password do not spell a word after you remove any non-alphabetical or special characters. The system checks all of the letters of the password together. Details...*

*This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).*

**Additional Policies**
- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.
**Password Requirements**

Adhere to the following password requirements, when selecting your Andrew account password:

<table>
<thead>
<tr>
<th>Must Contain</th>
</tr>
</thead>
<tbody>
<tr>
<td>• At least 8 characters.</td>
</tr>
<tr>
<td>• At least one uppercase alphabetic character (e.g., A-Z).</td>
</tr>
<tr>
<td>• At least one lowercase alphabetic character (e.g., a-z).</td>
</tr>
<tr>
<td>• At least one number (e.g., 0-9).</td>
</tr>
<tr>
<td>• At least one special character (e.g., ~!@#$%^&amp;*()_+=).</td>
</tr>
</tbody>
</table>

- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., ~!@#$%^&*()_+=).

Remove any non-alphabetical or special characters. The system checks all of the letters of the password together. [Details...](#)

*This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).

**Additional Policies**

- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.
Password Requirements

Adhere to the following password requirements, when selecting your Andrew account password:

**Must Contain**
- At least 8 characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., `~!@#$%^&()`_+-=).

**Additional Policies**
- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.
Can Long Passwords Be Secure and Usable?

Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor

Carnegie Mellon University
Prior: CHI 2011, Oakland 2012

- Examined policies including comp8, a typical strong policy
- Examined one “longer” policy, basic16
- Longer, simple passwords fairly usable and strong after many guesses
- But some very easily guessed
Study Objective

• Investigate password policies that
  • Take advantage of length
  • Are not too complicated
  • Prevent easily guessable passwords
Question: Metrics

• What metrics should we look at for meeting our objectives?
Strength Metrics

• Percent of passwords guessed after $10^6$ & $10^{12}$ guesses
Usability Metrics

- Sentiment
  - Creation difficulty, recall difficulty
- Time
  - Password creation and recall
- Memorability
  - Recall attempts, password writedown
Study Overview

- Two-part Mechanical Turk study
- Compensation:
  - 55 cents for part-one, 70 for part-two
- 8,143 participants finished both
Study walkthrough

Instructions
Create Pass
Survey I
Part I Recall

Wait 2 days
Email Invite
Part II Recall
Survey II
“Imagine that your main email service provider has been attacked. You need to use a new password for your email account, since your old password may be known by the attackers.”
Study walkthrough

Instructions

Create Pass

Survey I

Part I Recall

Password requirements:

- Include at least 16 characters

You may use letters, numbers, spaces, and other symbols in your password.

Choose a password:

Re-enter your password:

Continue
Study walkthrough

Instructions

Create Pass

Survey I

Part I Recall

1. Creating a password that meets the requirements given in this study was annoying.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Creating a password that meets the requirements given in this study was difficult.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Study walkthrough

Instructions

Create Pass

Survey I

Part I Recall

Please enter your password.
Study walkthrough

Wait 2 days

Email Invite

Part II Recall

Survey II
Study walkthrough

Log in to the Carnegie Mellon

To continue to the survey, please enter the password

I forgot my password
Study walkthrough

1. How did you just enter your password for this study?

- I used the "I forgot my password" link
- My browser automatically filled it in
- I copied and pasted it
- I typed it in from memory
- I used a password manager
- I looked it up and typed it in
- I prefer not to answer
- Other

Wait 2 days
Email Invite
Part II Recall
Survey II
Conditions

• 8 conditions

• each with a different password policy

• Between subjects, assigned round-robin
• Based on the CMU policy
• Represents typical strong password policy
• 8 characters
• Letters can’t form dictionary word
• Uppercase, lowercase, digit, symbol

AWordPass1!
1!WordWordWord
basic 12, basic 16, basic 20

- Require 12, 16, 20 characters
- Study length as the only requirement for strength
- Prior work has examined basic 16

passwords
passwordpassword
password passwordpass
3class12, 3class16

- Study both length and class requirement
- 12, 16 characters
- 3 of uppercase, lowercase, digit, symbol

CMUpassword1
passCMUpassword1
2word12, 2word16

- Encourage a passphrase
- 12, 16 characters
- Letters separated by a non-letter

password@cmu
password@cmupass
Results: Security
Password Strength

• Generated guess number for each password, up to a cutoff (Kelley et al. Oakland 2012)

• Used a context-free-grammar based cracker (Weir et al. IEEE SP 2009) tuned per condition

• Results presented as percent guessed by log number of guesses
Guessing curves by condition

- 2word12
- 2word16
- 3class12
- 3class16
- basic12
- basic16
- basic20

Percent Guessed vs. Guess Number chart.
comp8 outperforms 2word12 & basic
1% vs 2-5%
Prior graph to $10^6$
Remaining conditions all significantly better than comp8 at cutoff
24% vs 1-16%
Usability Results
Creation Difficult

comp8

basic12

basic16

basic20

3class12

3class16

2word12

2word16

Agreement

Disagreement

0%

100%
<table>
<thead>
<tr>
<th>comp8</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>basic12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>% cracked</td>
<td>$10^6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Column</td>
<td>% cracked 10^6</td>
<td>% cracked cutoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>-----------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>comp8</strong></td>
<td>0.6</td>
<td>23.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>------------------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td>93.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td>93.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part I</td>
<td>% creation difficult</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>comp8</strong></td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td>93.9</td>
<td>28.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td>93.9</td>
<td>34.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td>% creation difficult</td>
<td>part 2 recall tries</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td><strong>comp8</strong></td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td>93.9</td>
<td>28.9</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td>93.9</td>
<td>34.7</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td>% creation difficult</td>
<td>part 2 recall tries</td>
<td>entry time (sec.)</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td>13.2</td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td>11.6</td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td>93.9</td>
<td>28.9</td>
<td>1.3</td>
<td>13.7</td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td>93.9</td>
<td>34.7</td>
<td>1.3</td>
<td>15.3</td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.1</td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>14.6</td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td>14.8</td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
<tr>
<td>What would you choose?</td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part1</td>
<td>% creation difficult</td>
<td>part2 recall tries</td>
<td>entry time (sec.)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td>13.2</td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td>11.6</td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>12.4</td>
<td>93.9</td>
<td>28.9</td>
<td>1.3</td>
<td>13.7</td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>7.1</td>
<td>93.9</td>
<td>34.7</td>
<td>1.3</td>
<td>15.3</td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.1</td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>14.6</td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td>14.8</td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
<tr>
<td></td>
<td>% cracked 10^6</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td>% creation difficult</td>
<td>part2 recall tries</td>
<td>entry time (sec.)</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td>13.2</td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td>11.6</td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13.7</td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15.3</td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.1</td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>14.6</td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td>14.8</td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td>% creation difficult</td>
<td>part2 recall tries</td>
<td>entry time (sec.)</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td>13.2</td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td>11.6</td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.7</td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>15.3</td>
</tr>
<tr>
<td>2word12</td>
<td>2.1</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.1</td>
</tr>
<tr>
<td>2word16</td>
<td>1.0</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>14.6</td>
</tr>
<tr>
<td>3class12</td>
<td>1.5</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td>14.8</td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
<tr>
<td></td>
<td>% cracked $10^6$</td>
<td>% cracked cutoff</td>
<td>% finished part 1</td>
<td>% creation difficult</td>
<td>part 2 recall tries</td>
<td>entry time (sec.)</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>comp8</td>
<td>0.6</td>
<td>23.5</td>
<td>83.0</td>
<td>32.6</td>
<td>1.4</td>
<td>13.2</td>
</tr>
<tr>
<td>basic12</td>
<td>3.9</td>
<td>24.5</td>
<td>94.5</td>
<td>14.9</td>
<td>1.3</td>
<td>11.6</td>
</tr>
<tr>
<td>basic16</td>
<td>5.2</td>
<td>22.7</td>
<td>92.0</td>
<td>20.9</td>
<td>1.3</td>
<td>13.7</td>
</tr>
<tr>
<td>basic20</td>
<td>3.9</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>15.3</td>
</tr>
<tr>
<td>2word12</td>
<td>1.0</td>
<td>16.0</td>
<td>92.0</td>
<td>25.4</td>
<td>1.4</td>
<td>14.6</td>
</tr>
<tr>
<td>2word16</td>
<td>1.5</td>
<td>6.6</td>
<td>92.1</td>
<td>35.2</td>
<td>1.4</td>
<td>14.8</td>
</tr>
<tr>
<td>3class12</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
<tr>
<td>3class16</td>
<td>0.3</td>
<td>1.4</td>
<td>90.5</td>
<td>40.5</td>
<td>1.4</td>
<td>16.2</td>
</tr>
</tbody>
</table>

**3class12 more usable during creation than 2word16**
Meeting Requirements

• Prior work speculated users meet requirements in predictable, minimal ways (e.g., NIST 06)

• This was not true in some cases
Exceeding Length Requirement

66% made a longer password than required
Exceeding Length Requirement

% cracked:
not exceeding and exceeding minimum length

Exactly Met
Exceeded
Exceeding Character Class Requirement

64% used more classes than required, ignoring comp8 that needed to use all four
Exceeding Character Class Requirement

% cracked:
not exceeding and exceeding minimum char classes
Common Substrings in Cracked Passwords

Certain substrings within passwords were a hallmark of more easily cracked passwords
Common Substrings

<table>
<thead>
<tr>
<th>containing</th>
<th>1234</th>
<th>4.2%</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td></td>
<td>3.1%</td>
</tr>
<tr>
<td>this</td>
<td></td>
<td>1.7%</td>
</tr>
<tr>
<td>turk</td>
<td></td>
<td>1.6%</td>
</tr>
</tbody>
</table>
## Common Substrings

<table>
<thead>
<tr>
<th>Substring</th>
<th>Containing</th>
<th>% Cracked with</th>
<th>% Cracked without</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>4.2%</td>
<td>44%</td>
<td>13%</td>
</tr>
<tr>
<td>password</td>
<td>3.1%</td>
<td>45%</td>
<td>14%</td>
</tr>
<tr>
<td>this</td>
<td>1.7%</td>
<td>23%</td>
<td>14%</td>
</tr>
<tr>
<td>turk</td>
<td>1.6%</td>
<td>37%</td>
<td>14%</td>
</tr>
</tbody>
</table>
Common Substrings

<table>
<thead>
<tr>
<th>Password</th>
<th>% Cracked with</th>
<th>% Cracked without</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>3.1%</td>
<td>45%</td>
</tr>
<tr>
<td>password</td>
<td>1.7%</td>
<td>23%</td>
</tr>
<tr>
<td>this</td>
<td>1.6%</td>
<td>37%</td>
</tr>
<tr>
<td>turk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Our study was on mechanical *turk*. Yahoo password set has *yahoo* passwords.
Limitations

• What do you think they were?
Limitations

• Only test recall after 5 minutes & 2 days
• Passwords not protecting actual value
  • Recent work showed MTurk workers make similar passwords to real users (CCS 2013)
Conclusion

• Longer password policies can be more usable, sometimes more secure, than traditional “strong” policies

• 3class12, 2word16 emerged as promising

• Patterns emerged in cracked passwords