04. Passwords

Blase Ur and Mainack Mondal
April 4th, 2018
CMSC 23210 / 33210
Google security exec: 'Passwords are dead'

Speaking at TechCrunch Disrupt, Google's Heather Adkins says startups should look beyond passwords to secure users and their data.

PCWorld

Yahoo wants to kill the password one text message at a time

Computerworld

Russian credential theft shows why the password is dead

It's way past time for companies to implement strong authentication measures.

The Guardian

Google aims to kill passwords by the end of this year

Gizmodo

The Tech That Will Kill Passwords

Adam Clark Estes
12/04/14 2:30pm · Filed to: PASSWORDS
Why Passwords?

• Familiar to people
• Nothing to carry
• Difficult to coerce
• Easy to deploy, revoke, and replace
Threats to Password Security

- Online attack against live system
Threats to Password Security

• Online attack against live system
  – Rate-limiting
Threats to Password Security

- Online attack against live system
- Attack against password-protected file
- Offline attack against stolen database
Anatomy of an Offline Attack

• Attacker compromises database
  – hash(“Blase”) = $2a$04$iHdEgkI681VdDMc3f7edau9phRwORvhYjqWAIb7hb4B5uFJ01g4zi$

• Attacker makes and hashes guesses
• Finds match → try on other sites
### Problem 1: Absurd Advice

**Carnegie Mellon University**

**Password Requirements**

<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;*()?&gt;&lt;./_+-=).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cannot Contain</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Known information (i.e., first name, last name, Andrew user ID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).</td>
</tr>
<tr>
<td>- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*</td>
</tr>
<tr>
<td>- A word that is found in a standard dictionary.*</td>
</tr>
<tr>
<td>(after removing non-alpha characters).</td>
</tr>
</tbody>
</table>

*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.
Problem 2: Inaccurate Feedback

Password1!
Problem 3: Unhelpful Feedback

Please enter a stronger password.

Please enter a stronger password.
1. Impact of password meters
2. Modeling password cracking
3. Password perceptions
4. Neural-network-based guessing
5. Building a data-driven meter
Meters’ Security & Usability Impact

Meters Are Ubiquitous
Test Meters’ Impact

• How do meters impact password security?
• How do meters impact usability?
  – Memorability
  – User sentiment
  – Timing
• What meter features matter?
• 2,931-participant online study
Create a password
Account Password

A strong password helps prevent unauthorized access to your email account.

Type new password: ******

8-character minimum; case sensitive

Password strength: Bad. Consider adding an uppercase letter or making your password longer.

Retype new password:

- Make my password expire every 72 days.

Save
### Visual Differences

| Type new password: | ![Password Meter]
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baseline meter</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td><strong>Three-segment</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td><strong>Green</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td><strong>Tiny</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td><strong>Huge</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td><strong>No suggestions</strong></td>
<td>Fair.</td>
</tr>
<tr>
<td><strong>Text-only</strong></td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
</tbody>
</table>
Visual Differences

Type new password: useniX

8-character minimum; case sensitive

Baseline meter: Fair. Consider adding a digit or making your password longer.

Three-segment: Fair. Consider adding a digit or making your password longer.

Green: Fair. Consider adding a digit or making your password longer.

Tiny: Fair. Consider adding a digit or making your password longer.

Huge: Fair. Consider adding a digit or making your password longer.

No suggestions: Fair.

Text-only: Fair. Consider adding a digit or making your password longer.
Scoring Differences

Type new password: usenIX$e5
8-character minimum; case sensitive

Baseline meter: Excellent!

Half-score: Poor. Consider adding a different symbol or making your password longer.

One-third-score: Bad. Consider adding a different symbol or making your password longer.

Nudge-16: Poor. Consider making your password longer.

Nudge-Comp8: Excellent!
Key Results

• Stringent meters with visual bars increased resistance to guessing
• Visual differences did not significantly impact resistance to guessing
• No significant impact on memorability
Modeling Password Cracking

Password-Strength Metrics

• Statistical approaches
  – Traditionally: Shannon entropy
  – Recently: $\alpha$-guesswork

• Disadvantages for researchers
  – Usually no per-password estimates
  – Huge sample required
  – Not real-world attacks
Parameterized Guessability

• How many guesses a particular cracking algorithm with particular training data would take to guess a password
j@mesb0nd007!

Guess # 366,163,847,194
Guess # past cutoff
Guessability in Practice
Guessability in Practice
Single Cracking Approach
Default Configuration
Questions About Guessability

1) How does guessability used in research compare to an attack by professionals?
2) Would substituting another cracking approach impact research results?
Approach

4 password sets

- password
- iloveyou
- teamo123
- ...

- passwordpassword
- 1234567812345678!
- 1@2#3$4%5^6&7*8
- ...

- Pa$$w0rd
- iLov3you!
- 1QaZ2W@x
- ...

- pa$$word1234
- 12345678asDF
- !q1q!q1q!q1q
- ...

5 approaches

- hashcat
- advanced password recovery

- John the Ripper

- Kore Logic

SECURITY
Key Results

• Configuration is critical
• Considering single approach insufficient
  – Multiple approaches proxy for pros
• Analyses of password sets robust
  – More granular analyses not robust
Per-Password Highly Impacted

Password!

33
Per-Password Highly Impacted

• JTR guess # 801

Password!
Per-Password Highly Impacted

• JTR guess # 801
• Not guessed in $10^{14}$ PCFG guesses

Password!
Per-Password Highly Impacted

- JTR guess # 801
- Not guessed in $10^{14}$ PCFG guesses

Password!
Password Guessability Service

• Guessability of plaintext passwords

```
asdfF123#
P@ssw0rd!
Qwertyuiop!1
...```

https://pgs.ece.cmu.edu

```
"Guess ", "Password"
"127188816", "Qwertyuiop!1"
"1853004462", "asdfF123#"
"2251762491", "P@ssw0rd!"
...```

FREE!
The Art of Password Creation

Reverse-Engineering Passwords

~Cowscomehom3

“till the cows come home”
Key Results

• Character substitutions both infrequent and predictable
• Words and phrases frequently used
  – Wikipedia excellent source of training data
• Composition policy detrimental for some
Understand Origin of Passwords

LEFTbrown8!
Understand Origin of Passwords

LEFTbrown8!
Understand Origin of Passwords

LEFTbrown8!
Understand Origin of Passwords

LEFTbrown8!
Key Results

• Important misconceptions
  – Digits and symbols
  – Keyboard patterns
  – Dictionary words

• Misallocation of effort in password creation
Perceptions of Password Security

Perception vs. Reality
Compare actual strength of passwords to users’ perceptions.
Measuring Perceptions

• Online study
  – Compensated $5 for ~30 minutes

• 165 participants from Mechanical Turk
  – Age 18+, live in United States
  – Median age 33
  – 49% female, 51% male
  – 16% CS or related degree or job
  – 4% student/professional in computer security
Study Tasks

1. Evaluating password pairs
Study Tasks

1. Evaluating password pairs

Evaluating password pairs

\[ \text{p@ssw0rd} \quad \text{pAssw0rd} \]

\[ \begin{array}{c}
\text{p@ssw0rd} \\
\text{much more secure}
\end{array} \quad \begin{array}{c}
pAssw0rd \\
\text{much more secure}
\end{array} \]
1. Evaluating password pairs

Why?

p@ssw0rd

much more secure

pAssw0rd

much more secure
Task 1 Hypotheses

• 25 common characteristics, e.g.,
  – Capitalization
  – Letters vs. digits vs. symbols
  – Choice of words and phrases
Task 1 Hypotheses

• 25 common characteristics, e.g.,
  – Capitalization
  – Letters vs. digits vs. symbols
  – Choice of words and phrases

• Created 3 pairs per hypothesis
  – Randomly chose 1 pair per participant
Task 1 Hypotheses

• 25 common characteristics, e.g.,
  – Capitalization
  – Letters vs. digits vs. symbols
  – Choice of words and phrases

• Created 3 pairs per hypothesis
  – Randomly chose 1 pair per participant
  – At least one password per pair from
Study Tasks

1. Evaluating password pairs
2. Rating selected passwords
Study Tasks

1. Evaluating password pairs
2. Rating selected passwords

Please rate the security of the following password: rolltide

Please rate the memorability of the following password: rolltide
Study Tasks

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies
Study Tasks

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies
4. Describing attackers
   – Who, why, how
Results

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies
4. Describing attackers
Evaluating Password Pairs

iloveyou88

ieatkale88
Evaluating Password Pairs

iloveryou88  ieatkle88
Evaluating Password Pairs

iloveyou88  ieatkale88

Image Creative Commons by Jinx! (span112) on Flickr
Evaluating Password Pairs

iloveyou88  ieatkale88

4,000,000,000 × more secure!
Evaluating Password Pairs

brooklyn16  brooklynyqy
Evaluating Password Pairs

brooklyn16  brooklynqy
Evaluating Password Pairs

brooklyn16  brooklynyqy
Evaluating Password Pairs

brooklyn16  brooklynqy

300,000 × more secure!
Ways People Were Wrong

• Overstated security benefits of:
  – Digits
  – Character substitutions (e.g., a→@)
  – Keyboard patterns (e.g., 1qaz2wsx3edc)

• Did not recognize common words/phrases
Many Ways People Were Right

• Capitalize letters other than the first
• Put digits and symbols in middle, not end
• Use symbols rather than digits
• Avoid:
  – Common first names
  – Words related to account
  – Years and sequences
If perceptions of many individual characteristics are correct, then why do people make bad passwords?
Perceptions of Attackers
Perception: How Many Guesses?
Perception: How Many Guesses?

- 2 guesses (Min)
Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000 guesses (Max)
Perception: How Many Guesses?

- 2 guesses (Min)
- $10^{18}$ guesses (Max)
- $34\% \leq 50$ guesses (manual attack)
Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)
- 67% ≤ 50,000 guesses (small-scale)
Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)
- 67% ≤ 50,000 guesses (small-scale)
- 7% ≥ 10^{14} guesses (large-scale)
Reality: How Many Guesses?
Reality: Small-Scale Guessing
Reality: Small-Scale Guessing

- Targeted guessing by someone you know
Reality: **Small-Scale Guessing**

- Targeted guessing by someone you know
- Automated attack by a stranger
Reality: Small-Scale Guessing

• Targeted guessing by someone you know
• Automated attack by a stranger
  – Online: 1 – 1,000,000 guesses
Reality: Large-Scale Guessing
Reality: Large-Scale Guessing

- Against stolen database of passwords
Reality: Large-Scale Guessing

- Against stolen database of passwords
- Against password-protected file
Reality: Large-Scale Guessing

- Against stolen database of passwords
- Against password-protected file
- 1,000,000 guesses (best practices)
Reality: Large-Scale Guessing

- Against stolen database of passwords
- Against password-protected file
- $1,000,000$ guesses (best practices)
- $10^{14}$ or more (common reality)
Perception

Small-scale
67% ≤ 50,000

Reality

Small-scale…
…and large-scale
≥ 10^{14} guesses
Conclusions
Conclusions

• Perceptions of individual characteristics
  – Often consistent with current attacks
  – Some crucial differences
Conclusions

• Perceptions of individual characteristics
  – Often consistent with current attacks
  – Some crucial differences

• Huge variance in perceptions of attackers
Conclusions

• Perceptions of individual characteristics
  – Often consistent with current attacks
  – Some crucial differences
• Huge variance in perceptions of attackers
• Current user feedback is insufficient
Better Password Scoring

Better Password Scoring

• Real-time feedback
• Runs entirely client-side
• Accurately models password guessability
Generating Passwords
Generating Passwords

password → o or maybe 0 or O or ...
Generating Passwords

Next char is:
A: 3%
B: 1%
C: 0.6%
...
O: 55%
...
Z: 0.01%
0: 20%
1: ...
Generating Passwords

<table>
<thead>
<tr>
<th>Next char is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: 3%</td>
</tr>
<tr>
<td>B: 2%</td>
</tr>
<tr>
<td>C: 5%</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>O: 2%</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>Z: 0.2%</td>
</tr>
<tr>
<td>0: 1%</td>
</tr>
<tr>
<td>1: ...</td>
</tr>
<tr>
<td>END: 2%</td>
</tr>
</tbody>
</table>
Generating Passwords

Prob: 100%

Next char is:
A: 3%
B: 2%
C: 5%
...
O: 2%
...
Z: 0.2%
0: 1%
1: ...
END: 2%
Generating Passwords

“C”
Prob: 5%
Generating Passwords

“C”
Prob: 5%

Next char is:
A: 10%
B: 1%
C: 4%
...
O: 8%
...
Z: 0.02%
0: 3%
1: ...
END: 6%
Generating Passwords

"C"
Prob: 5%

Next char is:
A: 10%
B: 1%
C: 4%
...
O: 8%
...
Z: 0.02%
0: 3%
1: ...
END: 6%
Generating Passwords

“CA”
Prob: 0.5%

Next char is:
A: 3%
B: 10%
C: 7%
...
O: 1%
...
Z: 0.03%
0: 2%
1: ...
END: 12%
Generating Passwords

“CAB”
Prob: 0.05%

Next char is:
A: 3%
B: 10%
C: 7%
...
O: 1%
...
Z: 0.03%
0: 2%
1: ...
END: 3%
Generating Passwords

“CAB”
Prob: 0.05%

Next char is:
A: 4%
B: 3%
C: 1%
...
O: 2%
...
Z: 0.01%
0: 4%
1: ...
END: 12%
Generating Passwords

“CAB”
Prob: 0.05%

Next char is:
A: 4%
B: 3%
C: 1%
...
O: 2%
...
Z: 0.01%
0: 4%
1: ...
END: 12%
Generating Passwords

“CAB”
Prob: 0.006%
Generating Passwords

CAB - 0.006%
CAC - 0.0042%
ADD1 - 0.002%
CODE - 0.0013%
...


Design Space

• Model size: 3mb (browser) vs. 60mb (GPU)
• Transference learning
  – Novel password-composition policies
• Training data
  – Natural language
• (Many others)
Method

- Test on many password sets
- Monte Carlo methods to estimate guess #
Results

Percent guessed

60%
40%
20%
0%

Guesses

$10^1$  $10^4$  $10^7$  $10^{10}$  $10^{13}$  $10^{16}$  $10^{19}$  $10^{22}$  $10^{25}$
Results

More accurate guessing

Percent guessed:
- 60%
- 40%
- 20%
- 0%

Guesses:
- $10^1$
- $10^4$
- $10^7$
- $10^{10}$
- $10^{13}$
- $10^{16}$
- $10^{19}$
- $10^{22}$
- $10^{25}$
Neural Networks Guess Better
Neural Networks Guess Better

The graph shows the percent guessed against the log of the number of guesses. The curves represent different methods: MinGuess, Neural Markov, PCFG, and Hashcat. The neural network method consistently outperforms the others, reaching 100% accuracy with fewer guesses compared to the other methods.
Neural Networks Guess Better

![Graph showing the performance of different models in guessing percentages over guesses. The graph compares MinGuess, Neural Markov, PCFG, JTR, and Hashcat.](image)
Neural Networks Guess Better

Percent guessed

Guesses

10^1 10^4 10^7 10^{10} 10^{13} 10^{16} 10^{19} 10^{22} 10^{25}
Larger Model Not Major Advantage
Browser Implementation

- Start with smaller model
- Quantize parameters
- Lossless compression
- Pre-compute inexact mapping of probabilities → guess #
- Cache intermediate results
- <1mb, ~ 17ms per character
Intelligibility
Building a Data-Driven Meter

We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
Provide Intelligible Explanations

Unicorn

- 21 characteristics
- Weightings determined with regression

Don't use simple transformations of words or phrases (unicorns → Unicorn) vs. Capitalize a letter in the middle, rather than the first character.
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
Main Screen…

Username: blase

Password: ********

Don't reuse a password from another account! (Why?)

Your password must:
- Contain 12+ characters
- Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords
…Shows Requirements
…Emphasizes Avoiding Reuse
…Provides Abstract Advice

Create Your Password

Username
blase

Password

Show Password

Don't reuse a password from another account! (Why?)

Your password must:
- Contain 12+ characters
- Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords
After Requirements Are Met…

![Create Your Password form](image)

- Your password could be better.
  - Don’t use dictionary words or words used on Wikipedia
  - Consider inserting digits into the middle
  - Consider making your password longer

See Your Password With Our Improvements

How to make strong passwords
Displays Score Visually
…Provides Text Feedback

Create Your Password

Username
blase

Password
************

Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

See Your Password With Our Improvements

How to make strong passwords

Continue
...Gives Detail (Password Shown)
...Offers Explanations

Create Your Password

Username
blase

Password
CryptoUnicorn3!

Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

A better choice: C3ryptoUnicorn@

How to make strong passwords
Explanations Shown in Modal

Ways to Improve Your Password

CryptoUnicorn3

Show Password & Detailed Feedback

A better choice: C3ryptoUnicorn@

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto) Attackers use software that automatically guesses millions of words commonly found in dictionaries, wordlists, or other people’s passwords
- Consider inserting digits into the middle, not just at the end 38% of people also put digits at the end of the password
- Consider making your password longer than 14 characters In recent years, attackers have gotten much better at guessing passwords under 16 characters

How to make strong passwords

OK
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
Evaluation

• 2-part online study
  1) Create password; survey; recall password (48 hours later, send automated email)
  2) Recall password; survey
• 4,509 Mechanical Turk participants
  – Between-subjects
  – Full-factorial design along three dimensions
Dimension 1: Composition Policy

• 8+ characters (1class8)

password

• 12+ characters, 3+ classes (3class12)

Password1234
Dimension 2: Stringency

- Low
- Medium
- High
Dimension 2: Stringency

- Low  \(10^4\) guesses
- Medium  \(10^6\) guesses
- High  \(10^8\) guesses
Dimension 2: Stringency

- Low: $10^4$ guesses, $10^8$ guesses
- Medium: $10^6$ guesses, $10^{12}$ guesses
- High: $10^8$ guesses, $10^{16}$ guesses
Dimension 3: Feedback
No Feedback

Create Your Password

Username
blase

Password
************

Show Password & Detailed Feedback

Confirm Password

Continue
Create Your Password

Username
blase

Password

Confirm Password

Continue
Public (Non-Sensitive) Feedback

Create Your Password

Username
blase

Password

Show Password & Detailed Feedback

Confirm Password

Your password could be better.
- Don’t use dictionary words or words used on Wikipedia
- Consider inserting digits into the middle
- Consider making your password longer

See Your Password With Our Improvements

How to make strong passwords

Continue
Standard Feedback

Create Your Password

Username
blase

Password
CryptoUnicorn3|

Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto) [Why?]
- Consider inserting digits into the middle, not just at the end [Why?]
- Consider making your password longer than 14 characters [Why?]

A better choice: CryptoUnicorn@

How to make strong passwords
Standard Feedback

Create Your Password

Username
blase

Password
CryptoUnicorn3|

Show Password & Detailed Feedback

Confirm Password

Your password could be better.
- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)
- Consider inserting digits into the middle, not just at the end
- Consider making your password longer than 14 characters

A better choice: C3ryptoUnicorn@

How to make strong passwords
Standard Feedback

Create Your Password

Username
blase

Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)

A better choice: CRYPTOUNICORN@

Confirm Password

A better choice: CRYPTOUNICORN@

Continue

How to make strong passwords
Create Your Password

Username
blase

Password
CryptoUnicorn3|
Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)
- Consider inserting digits into the middle, not just at the end
- Consider making your password longer than 14 characters

How to make strong passwords

Standard, No Suggested Improvement
Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)

- Consider inserting digits into the middle, not just at the end

- Consider making your password longer than 14 characters

A better choice: C3ryptoUniCorn@

How to make strong passwords

Continue
Measure Password Guessability

Percent guessed vs. Guesses
Measure Password Guessability
Measure Password Guessability

Percent guessed

Guesses

0% 20% 40% 60%

$10^1$ $10^3$ $10^5$ $10^7$ $10^9$ $10^{11}$ $10^{13}$ $10^{15}$
Measure Password Guessability

Passwords harder to guess

Percent guessed

Guesses

10^1 10^3 10^5 10^7 10^9 10^{11} 10^{13} 10^{15}
Measure Password Guessability

Percent guessed

Guesses

1c8–None
Feedback → More Secure Passwords

![Graph showing the percent guessed over guesses for two different password types, 1c8–None and 1c8–Bar–M. The graph illustrates that 1c8–None is more secure than 1c8–Bar–M as it takes more guesses to reach the same percent guessed.]
Feedback → More Secure Passwords

The graph shows the percent of passwords guessed over a range of guesses.

Three conditions are compared:
- 1c8-None
- 1c8-Bar-M
- 1c8-Std-M

The x-axis represents the number of guesses, and the y-axis represents the percent of passwords guessed.
Feedback → More Secure Passwords

- 1c8–None
- 1c8–Bar–M
- 1c8–Std–M
- 3c12–None
- 3c12–Bar–M
- 3c12–Std–M
Usability Results

• Feedback did not significantly impact password memorability
• More feedback → more difficult, annoying
• All features had value for some participants
Feedback → More Secure Passwords

https://github.com/cupslab/password_meter

• Help us improve the meter
• Demo: https://cups.cs.cmu.edu/meter

Blase Ur, Assistant Professor, University of Chicago