On the Usability and Security of Password-Based User Authentication

Maximilian Golla

Thesis Defense, Bochum, Germany, May 29, 2019
User Authentication

Competing requirements of security and usability. [1]

Common Factors:
- Knowledge (Password, PIN)
- Biometrics (Fingerprint, Face)
- Possession (Security Key)

Reinforced by:
- 2-Factor Authentication
- Risk-based Authentication

Passwords Are Not Dead

Primary means of authentication on the Web. [2]

- Accounts: ~24
- Passwords: 6-8

[Ref. 2] Sarah Pearman et al.: Let’s Go in For a Closer Look: Observing Passwords in Their Natural Habitat. (CCS ‘17)
Overview

Thesis

- **Password Management**
  - CCS 16

- **Password Strength**
  - CCS 18, SP 19

- **Password Recovery**
  - PW 15, NDSS 17, USEC 19

- **Password Reuse**
  - CCS 18

- **Mobile Authentication**
  - USEC 17, USEC 19, CCS 19*

- **Access Control**
  - USENIX Sec. 18

*Under review

**Workshops:** Rate-Limiting, Semantics of Passwords, Strength Meter
Overview

Today

Password Management
- CCS 16

Password Strength
- CCS 18, SP 19

Mobile Authentication
- USEC 17, USEC 19, CCS 19*

Password Recovery
- PW 15, NDSS 17, USEC 19

Password Reuse
- CCS 18

Access Control
- USENIX Sec. 18

Workshops: Rate-Limiting, Semantics of Passwords, Strength Meter

[*] Under review
Outline

- Introduction
- Strength Meter
- Reuse Notifications
How Users Choose Passwords

- Well-defined process
- Misconceptions in mental model
  “Adding ‘!’ to the end instantly makes it secure.” [3]
- Estimating strength not easy

[Ref. 3] Ur et al.: “I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab. (SOUPS ‘15)
Estimating the Strength of a Password is Tough

“Adding ‘!’ to the end instantly makes it secure.” [3]

Password 1: iloveyou88
Password 2: ieatkale88

Options:
A. Password 1 is stronger
B. Password 2 is stronger
C. They are equally strong

[Ref. 3] Ur et al.: “I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab. (SOUPS ‘15)
Estimating the Strength of a Password is Tough

“Adding ‘!’ to the end instantly makes it secure.” [3]

Password 1: iloveyou88
Guess Number: $1.5 \times 10^4$

Password 2: ieatkale88
Guess Number: $3.1 \times 10^9$

[Ref. 3] Ur et al.: “I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab. (SOUPS ’15)
Support Users in Choosing Secure Passwords

Password  Strong  

Strength Meter
But They Are Not Always Accurate
How to Measure Accuracy?

**Reference**

<table>
<thead>
<tr>
<th>Top</th>
<th>Count</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,044,164</td>
<td>123456</td>
</tr>
<tr>
<td>2</td>
<td>176,120</td>
<td>password</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>1000</td>
<td>45,682</td>
<td>Baseball1</td>
</tr>
</tbody>
</table>

**Strength Meter**

Password: 123456

- Weak

Ranking:

1
2
3

- Ranking:
LUDS-based Meter:

Strong Password1

L: ✔️ U: ✔️ D: ✔️ S: ✗

Change password
It's a good idea to use a strong password that you're not using elsewhere

Current

New: ********
Password strength: Weak

Re-type new

Forgot your password?

Save Changes

Weak linkedin
Weak password
Weak 111111
Weak sunshine
Weak michael
Weak abdullah
Weak 666666
Medium 123456789
Medium 12345678
Weak thiago
Weak superman
Weak samson
Weak sammy1
Weak sailing
Strong Password1
Weak myaccount
Weak murphy
# Password “Strength”

<table>
<thead>
<tr>
<th>Meter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Text</strong></td>
<td>Weak, Medium, Strong</td>
</tr>
<tr>
<td><strong>Colors</strong></td>
<td>Red, Orange, Green</td>
</tr>
<tr>
<td><strong>Percentages</strong></td>
<td>42%</td>
</tr>
<tr>
<td><strong>Scores</strong></td>
<td>1-5</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>12 d, 9h, 47m</td>
</tr>
<tr>
<td><strong>Entropy</strong></td>
<td>82 bits</td>
</tr>
<tr>
<td><strong>Guess number</strong></td>
<td>1 018 291 guesses</td>
</tr>
</tbody>
</table>

**Reference:** Guess number

**Meter:** ???
Simulation Dataset

<table>
<thead>
<tr>
<th>LinkedIn</th>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Password</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>1 044 164</td>
<td>123456</td>
</tr>
<tr>
<td>176 120</td>
<td>password</td>
</tr>
<tr>
<td>88 076</td>
<td>12345678</td>
</tr>
<tr>
<td>78 720</td>
<td>111111</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>356</td>
<td>charlie22</td>
</tr>
<tr>
<td>356</td>
<td>mickey7</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>1</td>
<td><del>!@#$%^</del>!@</td>
</tr>
</tbody>
</table>
Simulate Common Errors Observed in Real-World Meters

Reference

Meter

Random sampling

Monotonic Transformations
Quantization
Disturbances
After: Quantized Output

<table>
<thead>
<tr>
<th>Reference</th>
<th>Meter</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>40</td>
</tr>
<tr>
<td>19</td>
<td>30</td>
</tr>
<tr>
<td>9</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>(Count)</td>
<td>(Bin)</td>
</tr>
</tbody>
</table>

- Weak
- Medium
- Good
- Strong
Result: Compare Weighted Ranking

Recommendation:
• Compare relative ranking only
• Weight passwords by importance

Weighted and ranked metrics (e.g., weighted Spearman correlation)

What can we do with this information?

Large-Scale Comparison
81 implementations
• Academia
• Websites
• PW Manager
• Operating Systems
• Previous Work

password-meter-comparison.org
Outline

Introduction

Strength Meter

Reuse Notifications
";'--have i been pwned?"

Check if you have an account that has been compromised in a data breach

Email address

Pwned? 7,858,347,021

Pwned websites

95,745

Pastes

117,180,866

Paste accounts
Reuse Attacks?

<table>
<thead>
<tr>
<th>Email</th>
<th>Cracked SHA-1</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>Hiking91</td>
</tr>
<tr>
<td><a href="mailto:joe@mail.com">joe@mail.com</a></td>
<td>R0cky!17</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>ILoveBananas!</td>
</tr>
</tbody>
</table>

I used “R0cky!17” everywhere!

1 guess can be enough!

<table>
<thead>
<tr>
<th>Email</th>
<th>Secure Argon2i Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:joe@mail.com">joe@mail.com</a></td>
<td>$argon2i$v=19$m=4096,...</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

AcmeCo
Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

By Katie Collins | November 9, 2016 12:56 PM PST

For a data-saturated company of its size and scope, Facebook has markedly managed to avoid the kind of security scandals, breaches and hacks that have affected many other major web companies.

Take a closer look, and you'll see why. Though on the surface all seems calm, below the waves the social network is kicking its legs frantically and working around the clock to keep users' accounts safe.

Keeping Facebook safe and keeping it secure are two different things, the social network's chief security officer, Alex Stamos, said Wednesday at Web Summit in Lisbon. Security is about building walls to keep out threats and shore up defenses, but according to Stamos, safety is bigger than that.

"It turns out that we can build perfectly secure software and yet people can still get hurt," he said.

*The reuse of passwords is the No. 1 cause of harm on the Internet,* says Facebook's Alex Stamos.

Brendan Moran/Getty Images
"Stolen From Another Site"

Keep your account secure

Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren’t aware of any suspicious activity on your account, but please change your password now to help keep it secure.

Learn More  Continue
Study 1: Previously Sent Notifications

- Understanding
- Feelings
- Actions
- Perceptions
  - Effectiveness
  - Delivery Method
  - Legitimacy

MTurk, 15min, 180 respondents, $2.50
“You've got e-mail! ... shall I deal with it now?”

Concerning and a priority
(83% very high or high)
“Should I worry?”

Proportion of Responses

Feelings

worried
afraid
anxious
annoyance
concerned
nervous
confusion
angry
surprised
safe
suspicious
irritating
frustrated
upset
relieved
curiosity

negative neutral positive

Bochum, May 29, 2019 | Thesis Defense ‘19
“Something happened and you need to click ‘OK’ to get on with things.” [%6]

What may have caused you to receive this notification?
[Multi select]

- 60% Account hacked
- 21% New device (false alarm)
- 21% Data breach
- 19% Reuse

[Ref. 6] by Johnathan Nightingale – Firefox Software Engineer at Mozilla; [Img 1.] Guy Fawkes by Carlotta Rosi - thecircle.com
Call a Spade a Spade!

Don’t mention reuse

LinkedIn (0 - 4% respondents)

Allude to reuse

Facebook and Instagram (48 - 56% respondents)

listed reuse as a cause for receiving this notification.
Incomplete Mental Models

“The chances of someone guessing that I use the same password are still incredibly low.” (R171)

Current password-reuse notifications:

- ✔️ cause concern
- ✗️ explain the situation
Study 2: Components of Notifications

Delivery Medium
- Push / In-App / Email

Incident
- Unrelated / Our /

Account Activity
- No suspicious / Suspicious /

Remediation
- Create new / Recommend

Other Accounts
- Change all /

Extra Actions
- Enable 2FA + Manager /
... Unhealthy Behavior

What would you do about it?

- 90% Change it
- 6% Keep it the same
- 4% Don’t know

What would your new password be?

- 68% Modified password
- 13% Reused password
- 11% Use manager/browser
- 6% Other
- 2% Completely new
Incomplete Mental Models

“The hack wasn't specific to this company so it doesn't worry me.”

(R69)

After seeing a reuse notification, users

- ✔️ would change password
- ✗ but ineffectively
- ✗ have incomplete mental models
Mockup

Create your Google Account

One account is all you need
One free account gets you into everything Google.

Take it all with you
Switch between devices, and pick up where you left off.

Password strength: Weak
Use at least 8 characters. Don’t use a password from another site, or something too obvious like your pet’s name. Why?

Choose your username
@gmail.com

Create a password

Safari detected that you are reusing a password.
Consider using this strong password instead.
funrux-Hommez-kajzo7
This password will be saved to your iCloud Keychain and will AutoFill on all your devices. Look up your saved passwords in Safari Passwords preferences or by asking Siri.

Gender
Conclusion

Passwords

Coping

Weak Passwords

Reused Passwords

Password Strength Meter

Password

Strong

Password

123456
password
123456789
qwerty
cookie
777777
00miner0
0031alice0031

Weight
1 044 164
176 120
136 179
48 229
19 554
15 423
88 076

Ranking
4.
3.
1.
2.
1.
3.
6.

Reference
1.
2.
3.
4.
5.
6.
7.

Strength Meter

Reuse Notifications