11. Authentication
Part 3
& Access Control

Blase Ur and David Cash
February 4th, 2022
CMSC 23200 / 33250
User-Centered Security
Some Ways to Understand Users

- Retrospective analysis of user-created password breaches
- Large-scale online studies
- Examine real passwords with permission
- Qualitative studies
How Do We Help Users Make Better Passwords?
Problem 1: Bad Advice

Carnegie Mellon University

Password Requirements

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.*

*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
Problem 3: Unhelpful Feedback

Twitter

Password:

* Please enter a stronger password.

* Please enter a strong password.
Proactive Strength Checking

- Initial idea: provide feedback
- In practice: complexities regarding what to model, and how to do so efficiently
Meters’ Security & Usability Impact

Meters Are Ubiquitous

- Brilliant
- Password Strength: Fair
- Password strength: Strong
- Weak
- Password could be more secure.
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

<table>
<thead>
<tr>
<th>Type new password:</th>
<th>Use <code>!</code></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

<table>
<thead>
<tr>
<th>Type new password:</th>
<th>usen1X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8-character minimum; case sensitive</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baseline meter</th>
<th>Fair. Consider adding a digit or making your password longer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three-segment</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Green</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Tiny</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Huge</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>No suggestions</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Text-only</td>
<td>Fair. Consider adding a digit or making your password longer.</td>
</tr>
</tbody>
</table>
Scoring Differences

Type new password: usenI$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
Authentication in Practice: Moving Towards A Passwordless World?
Case Study: WebAuthn

FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS

FIDO AUTHENTICATION: THE NEW GOLD STANDARD

- Protects against phishing, man-in-the-middle and attacks using stolen credentials
- Log in with a single gesture – HASSLE FREE!
- Already supported in market by top online services
Case Study: WebAuthn

- Created under the FIDO2 project, now a W3C standard
- Goal: Authenticate on web using public-key crypto
- Implemented in specialized hardware OR in software using a TPM/TEE
Case Study: WebAuthn

User interaction: Push a button on a key, type a PIN into the device, present biometric (fingerprint) to hardware reader.
Authentication in Practice: Password Add-Ons / Alternatives
Single Sign-On

Login with Facebook

OpenID®
Single Sign-On: Shibboleth

Diagram from https://docs.shib.ncsu.edu/docs/shibworks.html
For a good (long) explanation, see: https://www.switch.ch/aai/demo/
Two-Factor Auth
Physical Tokens / Smart Cards

• Codes based on a cryptographic key
  – Token manufacturer also knows the key

• What if there is a breach?
Authentication in Practice:
I Forgot My Password
Resetting Accounts

• I forgot my password!
• Send an email?
• Security questions?
• In-person verification?
• Other steps?
• (No backup)
Authentication in Practice: Password Managers
Password Managers

• Trust all passwords to a single master password (still a good idea in most cases)
  – Also trust software
  – Centralized vs. decentralized architectures
Authentication in Practice: Password Reuse 😞
Password Reuse-Based Attacks

People Reuse Passwords

R0cky!14

R0cky!17

American Airlines

facebook

Taobao.com

Adobe

123456

Microsoft

Rocky!16

YouTube

SONY

Google

PayPal

WELLS FARGO

1&1

Dropbox

R0ckyBox

R0ckyStar

R0cky!17
Memory-Hard Hash Function

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

Rate-Limiting Guessing

Password Strength Meter

- Consider inserting digits into the middle, not just at the end
- Make your password longer than 8 characters
- Consider using 1 or more symbols

Your password could be better.

A better choice: `a#D18cmccs`

How to make strong passwords
<table>
<thead>
<tr>
<th>Email</th>
<th>SHA-1 Hash of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jane@aol.com">jane@aol.com</a></td>
<td>7c4a8d09ca3762af61e595209</td>
</tr>
<tr>
<td><a href="mailto:jessey@gmx.net">jessey@gmx.net</a></td>
<td>5baa61e4c9b93f3f0682250b6</td>
</tr>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>7c222fb2927d828af22f59213</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>ba93664a90285b9ff18a7a081</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>b1b3773a05c0ed0176787a4f1</td>
</tr>
</tbody>
</table>
Crack All The Things!

$> \text{hashcat} -m\ 100\ -a\ 0\ \$\text{TARGET}\ \$\text{DICT}$

<table>
<thead>
<tr>
<th>Email</th>
<th>Cracked SHA-1 Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jane@aol.com">jane@aol.com</a></td>
<td>123456</td>
</tr>
<tr>
<td><a href="mailto:jessey@gmx.net">jessey@gmx.net</a></td>
<td>5baa61e4c9b93f3f0682250b6</td>
</tr>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>Canada4ever</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>R0cky!17</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>HikingGuy89</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Dead On Arrival

Email   Cracked
---   ----
...   ...
jim@mail.com   R0cky!17
...   ...

1 guess is enough!
Monitoring the Black Market

Welcome back, [Username]

TheRealDeal

Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

0 5.0000 / BTC 5.0000

In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.
Class Digital
Ships From Worldwide

Buy It Now

Favorite Question
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
Password-Reuse Notifications

Important information regarding your Haulz account

You must reset your password before you can continue

Your email was found in a list of user data from another service. We're temporarily preventing access to your account to protect it against unauthorized access, in case you've reused the same password on HaulzChat.

Your email address or profile URL

Enter your email address or profile URL

Request a password reset

Please update your Spotify password.

To update your Spotify account, we need your current password. This is to ensure your account is secure and that only you can access your music and other content.

Please update your Spotify account.

Please update your LinkedIn password.

An email was sent to you with instructions on how to update your LinkedIn password.

Please update your LinkedIn password.

To keep your account secure, please update your LinkedIn password.

To stop receiving LinkedIn notifications, click here.

LinkedIn

Someone May Have

Someone Else May Have

Someone has your password

Hi, Jane Doe,

Someone has your password.

Please update your account info today.

Someone has your password

Hi, Jane Doe,

Please update your account info today.

Someone May Have

Someone Else May Have

Someone has your password

Hi, Tom,

For your protection and the safety of your data, we have reset your password.

Reset Your Password | view as a webpage

For more information please contact Customer Care at https://support.carbonite.com/.
Authentication in Practice: Checking for Compromised Credentials
Checking for Compromised Credentials

https://www.zdnet.com/article/google-launches-password-checkup-feature-will-add-it-to-chrome-later-this-year/
Checking for Compromised Credentials

Under the hood: How Password Checkup helps keep your accounts safe

01
Whenever Google discovers a username and password exposed by a data breach, we store a strongly hashed and encrypted copy of the data.

We keep an unencrypted 2-byte hash prefix to partition the database.

We encrypt the full hash using a secret key known only to Google.

02
When you log in to a site you use, Password Checkup will send a strongly hashed and encrypted copy of your username and password to Google. This ensures that Google never learns your account details.

Google only learns an anonymous hash prefix of your account details.

Password Checkup encrypts your full account details using a secret key known only to you.

03
We use private set intersection with blinding to search through every unsafe username and password without revealing your account details, or anyone else's, during the process.

Password Checkup fetches an encrypted database of every unsafe username and password that shares the same anonymous hash prefix of your account details.

Password Checkup locally encrypts the result with a secret key known only to you.

04
The final check for whether your username or password was in a data breach is entirely local if your account details were exposed, you should change your password immediately.

Password Checkup locally searches if your username and password are encrypted. It can match any of the unsafe usernames and passwords in the encrypted database.

https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html
What about Biometrics?
Biometrics

- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)
Practical Challenges for Biometrics

- Immutable (can’t be changed)
- Potentially sensitive data
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time
Storing Biometrics: Templates
iPhone
Touch ID

Android
Face Unlock

*Images fair use from androidcentral.com, creativebits.org, and businessinsider.com.*
Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter their password
- Falls back to the password
- Face recognition can be tricked by a photo
- Fingerprint recognition can be tricked by a gummy mold
- Users find fingerprint unlock convenient, but do not particularly like face unlock
Authentication Conclusions

• Authentication is really hard!
  – Hard for system administrators
  – Hard for users

• Unfortunately, authentication is necessary
Access Control
Access Control: Basic Instantiation

• File permissions on UNIX:
  – Owner, Group, Others

• Useful commands
  – chown (change **owner** of a file)
    • chown blase:plantnerds rareplants.txt
  – chmod (change **modes** of a file)
    • chmod g+w rareplants.txt (**user** **group** others, add + or remove -, **read** **write** **execute**)
    • chmod 750 rareplants.txt (additive: 0 = nothing, 1 = execute, 2 = write, 4 = read)
Access Control

• Role-based access control
  – Authorization based on role (e.g., “UChicago student”)

• Attribute-based access control
  – Authorization based on attribute(s) (e.g., “Over 7 feet tall”)

• Context-based access control
  – Authorization decision depends on the context (e.g., time of day)