A Two-Decade Retrospective Analysis of a University’s Vulnerability to Attacks Exploiting Reused Passwords

Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, Blase Ur
People Reuse Passwords

princess123

Gmail

NETFLIX

Princ3ss123!

CHASE

Letmein!

querty1999

princess99

Princ3ss123!
People Reuse Passwords & Attackers Know

- princess123
- princess99
- querty1999
- princess123

- Princ3ss123!
- Letmein!
Create Password or Passphrase

You have already used this password before. Please choose a different one.
<table>
<thead>
<tr>
<th>Username</th>
<th>Hash of Password</th>
<th>Created</th>
<th>Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>weimf</td>
<td>hash(i&lt;3cats1234)</td>
<td>Sep 17, 2016</td>
<td>Jul 1, 2019</td>
</tr>
<tr>
<td>weimf</td>
<td>hash(i&lt;3cats2019!)</td>
<td>Jul 1, 2019</td>
<td>present</td>
</tr>
<tr>
<td>hszym</td>
<td>hash(p@nc@kes99)</td>
<td>Aug 15, 2018</td>
<td>present</td>
</tr>
<tr>
<td>julietteh</td>
<td>hash(Tiwchnt89)</td>
<td>Nov 10, 2017</td>
<td>Aug 23, 2019</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Part 1: Measurement of password reuse over the past 20 years

Part 2: Survey of users that reused a password on their university account
Finding credentials in leaked data

Generating guesses for university accounts

Checking guesses and protecting accounts

Surveying impacted users

227,976 Usernames
Sources of Credentials

- 450 individual service breaches
  - LinkedIn, Chegg, etc.

- 12 large breach compilations
  - Collection #1, Anti Public Combo List, etc.

Finding credentials in leaked data → Generating guesses for university accounts → Checking guesses and protecting accounts → Surveying impacted users
Finding credentials in leaked data

Generating guesses for university accounts

Checking guesses and protecting accounts

Surveying impacted users

username: nisenoff

nisenoff@uchicago.edu

nisenoff@cmu.edu

nisenoff

nisenoff99@gmail.com
Finding credentials in leaked data → Generating guesses for university accounts → Checking guesses and protecting accounts → Surveying impacted users

Password Tweaking Methods

- Heuristic algorithms
  - Das et al. [1]
  - Wang et al. [2]

- Deep learning
  - pass2path [3]

- Hashcat ruleset
  - Best64.rule [4]

---

password
Password
password! 
password123
p@ssw0rd
…

---

“Common” Password Guesses

LinkedIn1 → password1
LinkedIn1 → UChicago1
P@ssw0rd1234 → P@ssw0rd1234
## Historical Password Policies

<table>
<thead>
<tr>
<th></th>
<th>Time Period</th>
<th>Length</th>
<th>Character Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2015 - Present</td>
<td>12 - 19</td>
<td>3+</td>
</tr>
<tr>
<td></td>
<td>2010 - 2015</td>
<td>8 - 16</td>
<td>3+</td>
</tr>
<tr>
<td></td>
<td>Prior to 2010</td>
<td>8 - 16</td>
<td>2+</td>
</tr>
<tr>
<td><strong>Passphrase</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2016 - Present</td>
<td>18 - 32</td>
<td>1+</td>
</tr>
<tr>
<td></td>
<td>2014 - 2016</td>
<td>18 - 50</td>
<td>1+</td>
</tr>
</tbody>
</table>
Finding credentials in leaked data → Generating guesses for university accounts → Checking guesses and protecting accounts → Surveying impacted users

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>…</th>
</tr>
</thead>
<tbody>
<tr>
<td>nisenoff</td>
<td>letmein123</td>
<td>…</td>
</tr>
<tr>
<td>blase</td>
<td>qwerty123</td>
<td>…</td>
</tr>
<tr>
<td>mgolla</td>
<td>Monkey&lt;3</td>
<td>…</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

Credential Guesses

UChicago Password History Database
Finding credentials in leaked data → Generating guesses for university accounts → Checking guesses and protecting accounts → Surveying impacted users
Surveys were customized to show participants the sources of data used to guess their password

40 Participants
Ethical Considerations

- Approved by IRB
- Study design informed by discussions with
  a. IT Leadership (including the CIO)
  b. Provost’s office
  c. University’s communications team
  d. University’s general counsel
  e. Alumni association
- Minimizing access to password history database
- Password resets
12,247 correct guesses

based on password reuse
We Guessed at Least One Password For:

- **4.5%** of all users
- **6.5%** of users that we made a guess for
- **32.0%** of users with a uchicago.edu email in a data breach
We guessed the current password for 3,618 accounts
Correct Guesses Came From 71 Individual Service Breaches and All 12 Breach Compilations
The Number of Accounts That Use Reused Passwords Changes Over Time
Reused Passwords Can Stay Valid for a Long Time … Even Relative to When Data Breaches Happened

Linkedin

Number of Accounts

0 500 1000 1500

Data Breach Occurred
Data Breach Became Public
Password Reuse Is Being Exploited

Password resets due to suspicious activity

Data Breach Occurred
Data Breach Became Public
Passwords Were Often Created at the UChicago Before They Appeared in a Data Breach

Before Data Breach

5,398 passwords
valid only before data breach

Date of Data Breach

5,915 passwords
Valid before and after data breach

After Data Breach

934 passwords
Valid only after data breach
Data Breaches Impact Specific Groups of Users Differently

<table>
<thead>
<tr>
<th></th>
<th>LinkedIn</th>
<th>Chegg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>11.2%</td>
<td>41.4%</td>
</tr>
<tr>
<td>Faculty</td>
<td>54.3%</td>
<td>2.2%</td>
</tr>
</tbody>
</table>

Percentages out of the number of students and faculty for which we had at least one correct guess
Sunshine!
correctbatteryhorsestaple
i@mforg3tful!
инeedapassword

5F4DCC3B5AA765D61D8327DEB882CF99
482C811DA5D5B4BC6D497FFA98491E38
62099D23A9D9910879D67449D9E084ED
1C8F93D67A694EE1DE6363D20228DAC8

Plaintext 85.3%
Hashed 14.7%
Verbatim
Reuse
54.7%

Password	Password
password!
password123
p@ssw0rd
pa$$word

Tweaked
Passwords
45.3%
User Reactions and Experiences (n = 40)

● Users are aware they are reusing passwords
● Users know about some, but not all, relevant data breaches
● Some users were unaware they had accounts on sites that had suffered a data breach

“I didn't know that I even had a Chegg account…” (P2)
Recommendations for Organizations

- Implement processes to expire unused accounts.

- Using credential checking services when passwords are created isn’t enough.

- Promptly check high-risk (i.e., organization-related) breaches when they become public.

- Check for reuse of hashed and tweaked passwords in less common data breaches.
A Two-Decade Retrospective Analysis of a University’s Vulnerability to Attacks Exploiting Reused Passwords

- Password reuse was a major source of risk for UChicago
- Passwords can remain vulnerable for a long time
- Users know they are reusing their passwords, but may not know which data breaches impact them

Alexandra Nisenoff
Maximilian Golla
Miranda Wei
Juliette Hainline
Hayley Szymanek
Annika Braun
Annika Hildebrandt
Blair Christensen
David Langenberg
Blase Ur