The password thicket: technical and market failures in human authentication on the web

Joseph Bonneau  Sören Preibusch
{jcb82,sdp36}@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

WEIS 2010
The Ninth Workshop on the Economics of Information Security
Boston, MA, USA
June 7, 2010
Password authentication is losing viability

In Our Inbox: Hundreds Of Confidential Twitter Documents
by Michael Arrington on Jul 14, 2009
481 Comments

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>25</td>
<td>35</td>
<td>48</td>
<td>72</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users in</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>25</td>
<td>35</td>
<td>48</td>
<td>72</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Revenue</td>
<td>$0.</td>
<td>$0.</td>
<td>$400000.</td>
<td>$400000.</td>
<td>$9000000.</td>
<td>$1700000.</td>
<td>$53000000.</td>
<td>$62000000.</td>
<td></td>
</tr>
<tr>
<td>Total Yearly</td>
<td></td>
<td></td>
<td>$4400000.</td>
<td>$14000000.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td>30</td>
<td>45</td>
<td>60</td>
<td>78</td>
<td>120</td>
<td>197</td>
<td>275</td>
<td>345</td>
<td></td>
</tr>
<tr>
<td>People Cost</td>
<td>$1050000.</td>
<td>$1575000.</td>
<td>$2100000.</td>
<td>$2730000.</td>
<td>$4200000.</td>
<td>$6895000.</td>
<td>$9625000.</td>
<td>$12075000.</td>
<td></td>
</tr>
<tr>
<td>Org Cost sans</td>
<td>$2030000.</td>
<td>$30450000.</td>
<td>$4060000.</td>
<td>$60343750.</td>
<td>$8681250.</td>
<td>$12160000.</td>
<td>$18270000.</td>
<td>$25375000.</td>
<td></td>
</tr>
<tr>
<td>Gross Margin</td>
<td>$43950000.</td>
<td>$39330000.</td>
<td>$33570000.</td>
<td>$28496250.</td>
<td>$23415000.</td>
<td>$21340000.</td>
<td>$48445000.</td>
<td>$70995000.</td>
<td></td>
</tr>
<tr>
<td>Net Earnings</td>
<td>$28567500.</td>
<td>$25584500.</td>
<td>$21820500.</td>
<td>$18522562.5</td>
<td>$15219750.</td>
<td>$13871000.</td>
<td>$30189250.</td>
<td>$46146750.</td>
<td></td>
</tr>
<tr>
<td>Cost of Starting Cash</td>
<td>1,015</td>
<td>450000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Password authentication is losing viability

32.6m passwords may have been compromised in RockYou hack

RockYou, which provides widgets popular with MySpace and Facebook users, has been hacked and 32.6m users are being urged to change their passwords.

RockYou SQL injection hack
January 2010
Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

By MAIL FOREIGN SERVICE
Last updated at 2:09 AM on 6th March 2010

Facebook founder Mark Zuckerberg has been accused of hacking into the email accounts of rivals and journalists.

The CEO of the world's most successful social networking website was accused of at least two breaches of privacy in a series of articles run by Businessinsider.com.

As part of a two-year investigation detailing the founding of Facebook, the magazine uncovered what it claimed was evidence of the hackings in 2004.

In the first instance, it said that, when Zuckerberg discovered that Harvard's student newspaper The Crimson was planning on running an article on him in 2004, he used reporters' Facebook login to hack into their accounts.

In the second instance, the magazine claimed Zuckerberg hacked into the accounts of rivals at Harvard who accused him of stealing their idea for a social network. He then allegedly tried to sabotage the rival network they had set up.

Business Insider claimed that Zuckerberg learned The Crimson was planning to write an article on him when he was called in for an interview in 2004.

The newspaper was investigating allegations by other Harvard students that Zuckerberg had stolen their social networking idea - allegations that are now well-documented and became the subject of a $65 million legal suit.

Zuckerberg e-mail hacking
2005
Password authentication is losing viability

Twitter mass reset
February 2010
We’ve conducted experiments to try to determine typical users’ habits in the choice of passwords . . . The results were disappointing, except to the bad guy.

—Morris and Thompson, 1979
Conventional wisdom is gloomy

1. **Users can’t manage**
   - re-use
   - weak passwords
   - post-it notes
   - sharing

2. **Free alternatives hard**
   - graphical
   - cognitive

3. **2-factor too expensive**
   - hardware tokens
   - client certs
   - smartphone

4. **Single sign-on limited**
Conventional wisdom is gloomy

1. **Users can’t manage**
   - re-use
   - weak passwords
   - post-it notes
   - sharing

2. **Free alternatives hard**
   - graphical
   - cognitive

3. **2-factor too expensive**
   - hardware tokens
   - client certs
   - smartphone

4. **Single sign-on limited**
Conventional wisdom is gloomy

1. Users can’t manage
   - re-use
   - weak passwords
   - post-it notes
   - sharing

2. Free alternatives hard
   - graphical
   - cognitive

3. 2-factor too expensive
   - hardware tokens
   - client certs
   - smartphone

4. Single sign-on limited

Cronto
Conventional wisdom is gloomy

1. **Users can’t manage**
   - re-use
   - weak passwords
   - post-it notes
   - sharing

2. **Free alternatives hard**
   - graphical
   - cognitive

3. **2-factor too expensive**
   - hardware tokens
   - client certs
   - smartphone

4. **Single sign-on limited**
Password collection remains ubiquitous

prevention of password sharing amongst top US sites

Figure 1. Proportion of sites collecting passwords and amongst these of sites blocking password sharing. Ratios given for top $k$ US sites with $k$ up to 900. Bumps are artefacts of the increasing window size for the arithmetic mean.
Supply side of the market remains poorly understood

1. How does the user experience vary from site to site?
2. What implementation weaknesses exist?
3. Which circumstantial factors affect sites’ implementation choices?
4. How do sites’ security requirements affect their choices?
5. Why do websites choose to collect passwords?
Coarse classification of password deployment cases

Identity
Coarse classification of password deployment cases

E-commerce
Random study sample designed for depth, breadth
Site classification allows for feature overlap

<table>
<thead>
<tr>
<th>Feature</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>News displayed</td>
<td>15</td>
<td>0</td>
<td>49</td>
<td>64</td>
</tr>
<tr>
<td>Products for sale</td>
<td>4</td>
<td>50</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>Payment details stored</td>
<td>7</td>
<td>30</td>
<td>2</td>
<td>39</td>
</tr>
<tr>
<td>Social networking</td>
<td>28</td>
<td>1</td>
<td>2</td>
<td>31</td>
</tr>
<tr>
<td>Premium accounts available</td>
<td>17</td>
<td>3</td>
<td>8</td>
<td>28</td>
</tr>
<tr>
<td>Email accounts provided</td>
<td>17</td>
<td>0</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Discussion forums</td>
<td>16</td>
<td>1</td>
<td>2</td>
<td>19</td>
</tr>
</tbody>
</table>
1 enrolment
   - p. advice
   - data collected

2 login
   - data transmission

3 update
   - re-authentication
   - p. requirements

4 recovery
   - backup auth.
   - replacement

5 attacks
   - user probing
   - p. guessing
Complete evaluation of visible password security

1 enrolment
   - p. advice
   - data collected

2 login
   - data transmission

3 update
   - re-authentication
   - p. requirements

4 recovery
   - backup auth.
   - replacement

5 attacks
   - user probing
   - p. guessing
Complete evaluation of visible password security

1. enrolment
   - p. advice
   - data collected

2. login
   - data transmission

3. update
   - re-authentication
   - p. requirements

4. recovery
   - backup auth.
   - replacement

5. attacks
   - user probing
   - p. guessing
Complete evaluation of visible password security

1 enrolment
   - p. advice
   - data collected

2 login
   - data transmission

3 update
   - re-authentication
   - p. requirements

4 recovery
   - backup auth.
   - replacement

5 attacks
   - user probing
   - p. guessing

Request a new password
If you have forgotten your password you can order a new one here.
Fields marked with * are mandatory.

*Username (e-mail address)
Please enter Username or Password.

1 How do you want to receive your new password?
   * Send out new password via email

2 Validation image
Are you still having problems with the letters? Don't worry, we can help you. Click here

Enter the characters you see in the image into the field below.
If you can't see all the letters, just change the image by clicking here

3 Get new password
Submit

IKEA
Complete evaluation of visible password security

1 enrolment
   - p. advice
   - data collected

2 login
   - data transmission

3 update
   - re-authentication
   - p. requirements

4 recovery
   - backup auth.
   - replacement

5 attacks
   - user probing
   - p. guessing
Semi-automated human-in-the-loop evaluation

Mozilla Firefox v 3.5.8 with:

- Autofill Forms 0.9.5.2
- CipherFox 2.3.0
- Cookie Monster 0.98.0
- DOM Inspector 2.0.4
- Greasemonkey 0.8.20100211.5
- Screengrab 0.96.2
- Tamper Data 11.0.1
Findings

1. How does the user experience vary from site to site?
2. What implementation weaknesses exist?
3. Which circumstantial factors affect sites’ implementation choices?
4. How do sites’ security requirements affect their choices?
5. Why do websites choose to collect passwords?
Choose a Password, which you'll also enter each time you use this service. Your password should be 5-15 characters in length and shouldn't include punctuation, symbol characters or spaces.

**Important:** We'll record your User Name and Password EXACTLY as you type them, so make a note if you enter in upper and lower case.

Bare-bones password entry is universal

Advice rare and inconsistent
User experience varies considerably

<table>
<thead>
<tr>
<th>Advice</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use digits</td>
<td>9</td>
<td>6</td>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>Use symbols</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>Graphical strength indicator</td>
<td>9</td>
<td>0</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>Difficult to guess</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Not a dictionary word</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Change regularly</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td><strong>Any</strong></td>
<td><strong>18</strong></td>
<td><strong>8</strong></td>
<td><strong>7</strong></td>
<td><strong>33</strong></td>
</tr>
</tbody>
</table>

- Bare-bones password entry is universal
- Advice rare and inconsistent
Findings

1. How does the user experience vary from site to site?

2. What implementation weaknesses exist?

3. Which circumstantial factors affect sites’ implementation choices?

4. How do sites’ security requirements affect their choices?

5. Why do websites choose to collect passwords?
TLS deployment sparse and inconsistent

Facebook

Please enter a new password

Email: facebook@ucam.preibusch.net

New Password: (required)

Confirm Password: (required)

Change Password

Keep me logged in

Forgot your password?

Email

Password

Login

Sign Up

It's free and anyone can join

First Name:
Last Name:
Your Email:
New Password:

I am: Select Sex:
Birthday: Month: Day: Year:

Why do I need to provide this?

Sign Up

Facebook
### TLS Deployment

<table>
<thead>
<tr>
<th>TLS Deployment</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>10</td>
<td>39</td>
<td>10</td>
<td>59</td>
</tr>
<tr>
<td>Full/POST</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Inconsistent</td>
<td>14</td>
<td>6</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>None</td>
<td>23</td>
<td>4</td>
<td>34</td>
<td>61</td>
</tr>
</tbody>
</table>
No standard for password length
Dear Joseph Bonneau,

You requested us to send you your EasyChair login information. Please use the following data to log in to EasyChair:

User name: jbonneau
Password: -----

Best regards,
EasyChair Messenger.
Hello, jbonneau:

Thanks for using your Ticketmaster account.

This is a temporary password:  ---
Use this temporary password to login and reset your password again.

We hope you enjoy using your account!

Thanks,
The Ticketmaster Team
Hi jbonneau,

Someone requested that your Last.fm password be reset. If this wasn’t you, there’s nothing to worry about – simply ignore this email and nothing will change.

If you DID ask to reset the password on your Last.fm account, just click here to make it happen:
http://www.last.fm/?id=<userid>&key=<authentication-token>

Best Regards,
The Last.fm Team
No standard for password recovery

<table>
<thead>
<tr>
<th>Recovery Mechanism</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email only</td>
<td>32</td>
<td>42</td>
<td>46</td>
<td>120</td>
</tr>
<tr>
<td>Email plus personal knowledge</td>
<td>11</td>
<td>4</td>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>Personal knowledge only</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>None available</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email contents</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Original password (cleartext)</td>
<td>5</td>
<td>14</td>
<td>17</td>
<td>36</td>
</tr>
<tr>
<td>Temporary password</td>
<td>11</td>
<td>15</td>
<td>12</td>
<td>38</td>
</tr>
<tr>
<td>Reset link</td>
<td>29</td>
<td>18</td>
<td>20</td>
<td>67</td>
</tr>
</tbody>
</table>
The following errors were encountered

- You are only permitted to make four login attempts every 1 minute(s)

Return to Previous Page

Truthdig
Password guessing rarely prevented

Sign In

Too many tries!

If you forgot your password, you can get help finding it, or you can open a new account.

Cafe Press

- Timeout
- Lockout/forced reset
- CAPTCHA
Password guessing rarely prevented

Log in

Don't have an account? Create one.

To help protect against automated password cracking, please enter the words that appear below in the box (more info):

signsowned

Username: test
Password: 

☐ Remember me (up to 30 days)

Log in  E-mail new password

Wikipedia

- Timeout
- Lockout/forced reset
- CAPTCHA
Password guessing rarely prevented

<table>
<thead>
<tr>
<th>countermeasure</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPTCHA</td>
<td>11</td>
<td>2</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>timeout</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>reset</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>none</td>
<td>37</td>
<td>43</td>
<td>46</td>
<td>126</td>
</tr>
</tbody>
</table>
Password guessing rarely prevented

<table>
<thead>
<tr>
<th>limit</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>&gt; 100</td>
<td>37</td>
<td>43</td>
<td>46</td>
<td>126</td>
</tr>
</tbody>
</table>
Create an Account

Required information for Google account

Your current email address: [Your email address]

There's already a Google Account associated with this email address. Please sign in; or, if you forgot your password, reset it now. [?]
User probing prevention rarely complete

Sign In

E-mail: [redacted]
Password: [redacted]

Tick: Remember me on this computer

⚠️ Oops, unknown user email. Have you signed up yet?

Sign In

Forgot your password?
Ask

Enrolment
Login
Recovery
Request to Reset Your Password

Please fix the following errors:

- We're sorry, but that email address is not in our records. Please confirm your information is correct and try again.

Don't worry about forgetting your password, resetting it is quick and easy.

Just enter your email address:

[Input field]

Continue

Zappos!
### User probing prevention rarely complete

<table>
<thead>
<tr>
<th>interface</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enrolment</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>login</td>
<td>43</td>
<td>41</td>
<td>38</td>
<td>132</td>
</tr>
<tr>
<td>reset</td>
<td>11</td>
<td>7</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>all</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
### 10-dimensional password security policies

<table>
<thead>
<tr>
<th>feature</th>
<th>cardinality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrolment email contents</td>
<td>8</td>
</tr>
<tr>
<td>Password advice</td>
<td>16</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>8</td>
</tr>
<tr>
<td>Password requirements</td>
<td>16</td>
</tr>
<tr>
<td>Federated login support</td>
<td>8</td>
</tr>
<tr>
<td>Password update</td>
<td>8</td>
</tr>
<tr>
<td>Password recovery mechanism</td>
<td>8</td>
</tr>
<tr>
<td>Brute force restrictions</td>
<td>4</td>
</tr>
<tr>
<td>User probing restricted</td>
<td>12</td>
</tr>
<tr>
<td>TLS deployment</td>
<td>4</td>
</tr>
</tbody>
</table>
Most sites re-inventing the wheel

<table>
<thead>
<tr>
<th>Uniqueness radius</th>
<th>% of sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100.0</td>
</tr>
<tr>
<td>1</td>
<td>90.6</td>
</tr>
<tr>
<td>2</td>
<td>56.0</td>
</tr>
<tr>
<td>3</td>
<td>24.0</td>
</tr>
<tr>
<td>4</td>
<td>7.3</td>
</tr>
<tr>
<td>5</td>
<td>1.3</td>
</tr>
<tr>
<td>6</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Security-conscious sites are pioneers

<table>
<thead>
<tr>
<th>Score</th>
<th>Cluster of sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Identity site</td>
</tr>
<tr>
<td>1</td>
<td>E-commerce site</td>
</tr>
<tr>
<td>2</td>
<td>Content site</td>
</tr>
<tr>
<td>3</td>
<td>Payment</td>
</tr>
</tbody>
</table>

No TLS, no password requirements, password emailed, no guessing or user probing restrictions, email addresses verified

- No TLS, no password requirements, password emailed, no guessing or user probing restrictions, email addresses verified
- TLS deployed, 6 char. min. password, emailed reset links, no password advice, guessing restrictions in place, email addresses verified
- TLS deployed, 6 char. min. password, personal knowledge questions for reset, no password advice, no guessing or user probing restrictions, email addresses verified
- TLS deployed, 6 char. min. password, emailed reset links, no password advice, no guessing or user probing restrictions, email addresses not verified
- No TLS, 6 char. min. password, personal knowledge questions for reset, no password advice, no guessing or user probing restrictions, email addresses verified

J. Bonneau, S. Preibusch (U. of Cambridge)
Findings

1. How does the user experience vary from site to site?
2. What implementation weaknesses exist?
3. **Which circumstantial factors affect sites’ implementation choices?**
4. How do sites’ security requirements affect their choices?
5. Why do websites choose to collect passwords?
10-point aggregate password score used for analysis

<table>
<thead>
<tr>
<th>feature</th>
<th>scoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>enrolment</strong></td>
<td></td>
</tr>
<tr>
<td>Password selection advice given</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Minimum password length required</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Dictionary words prohibited</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Numbers or symbols required</td>
<td>+1 pt</td>
</tr>
<tr>
<td>User list protected from probing</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Cleartext password sent in email after enrolment</td>
<td>−1 pt</td>
</tr>
<tr>
<td><strong>login</strong></td>
<td></td>
</tr>
<tr>
<td>Password hashed in-browser before POST</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Limits placed on password guessing</td>
<td>+1 pt</td>
</tr>
<tr>
<td>User list protected from probing</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Federated identity login accepted</td>
<td>+1 pt</td>
</tr>
<tr>
<td><strong>password update</strong></td>
<td></td>
</tr>
<tr>
<td>Password re-entry required to authorise update</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Notification email sent after password reset</td>
<td>+1 pt</td>
</tr>
<tr>
<td><strong>password recovery</strong></td>
<td></td>
</tr>
<tr>
<td>Password update required after recovery</td>
<td>+1 pt</td>
</tr>
<tr>
<td>Cleartext password sent in email upon request</td>
<td>−1 pt</td>
</tr>
<tr>
<td>User list protected from probing</td>
<td>+1 pt</td>
</tr>
<tr>
<td><strong>encryption</strong></td>
<td></td>
</tr>
<tr>
<td>Full TLS for all password submission</td>
<td>+2 pts</td>
</tr>
<tr>
<td>POST only TLS for password submission</td>
<td>+1 pt</td>
</tr>
</tbody>
</table>
More popular sites do better

J. Bonneau, S. Preibusch (U. of Cambridge)

The password thicket

June 7, 2010 18 / 28
Popular, growing, competent sites are more secure

<table>
<thead>
<tr>
<th>Positive 3-mo. traffic change</th>
<th>Password score &gt; median</th>
<th>TLS deployed correctly</th>
<th>Guessing attacks restricted</th>
<th>Minimum password length enforced</th>
<th>Dictionary words prohibited</th>
<th>Cleartext passwords mailed</th>
<th>Notification of password reset</th>
<th>Email verified on enrolment</th>
<th>CAPTCHA required on enrolment</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ + +</td>
<td>↑ ↑ ↑</td>
<td>↑ ↑</td>
<td>↑ ↑</td>
<td>↑</td>
<td>+</td>
<td>+</td>
<td>↓</td>
<td>↓</td>
<td></td>
</tr>
<tr>
<td>Years online &gt; 10</td>
<td>+ + +</td>
<td>↓ ↓</td>
<td>+</td>
<td>↑</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load time &lt; med.</td>
<td>↑ +</td>
<td>↑ +</td>
<td>↑ +</td>
<td>↑ −</td>
<td>↑</td>
<td>↓ ↓ ↓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Traffic Rank > 25th %ile | ↑ ↑ ↑ | ↑ | + | + | ↑ ↑ | + |
| Traffic Rank > med. | ↑ ↑ ↑ | ↑ ↑ | + | ↑ ↑ ↑ | ↓ | ↑ | + | + |
| Traffic Rank > 75th %ile | ↑ ↑ ↑ | ↑ ↑ ↑ | ↑ | ↑ ↑ ↑ | ↓ | + | ↑ ↑ ↑ | ↑ |

| Industry Traffic Rank > 25th %ile | ↑ ↑ ↑ | + | + | ↑ | ↑ ↑ | + |
| Industry Traffic Rank > med. | ↑ ↑ ↑ | + | ↑ ↑ ↑ | ↑ ↑ ↑ | ↑ ↑ ↑ | ↑ ↑ |
| Industry Traffic Rank > 75th %ile | ↑ ↑ ↑ | ↑ | ↑ ↑ ↑ | ↑ ↑ ↑ | − | ↑ ↑ | + |

| Page Views > 25th %ile | ↑ ↑ ↑ | ↑ ↑ | ↑ ↑ | ↑ ↑ | ↑ ↑ |
| Page Views > med. | ↑ ↑ ↑ | ↑ ↑ | + | ↑ ↑ ↑ | ↓ | ↑ | + | + |
| Page Views > 75th %ile | ↑ ↑ ↑ | ↑ ↑ ↑ | + | ↑ ↑ ↑ | ↓ | ↑ | ↑ | ↑ ↑ |

J. Bonneau, S. Preibusch (U. of Cambridge)

The password thicket

June 7, 2010
Findings

1. How does the user experience vary from site to site?
2. What implementation weaknesses exist?
3. Which circumstantial factors affect sites’ implementation choices?
4. How do sites’ security requirements affect their choices?
5. Why do websites choose to collect passwords?
Content sites provide the least security

The password thicket

J. Bonneau, S. Preibusch (U. of Cambridge)
Payment-storing sites do it best

<table>
<thead>
<tr>
<th>Identity segment</th>
<th>TLS deployed correctly</th>
<th>Guessing attacks restricted</th>
<th>Minimum password length enforced</th>
<th>Dictionary words prohibited</th>
<th>Digits</th>
<th>Symbols</th>
<th>Cleartext passwords mailed</th>
<th>Notification of password reset</th>
<th>Email verified on enrolment</th>
<th>CAPTCHA required on enrolment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>+</td>
<td>↓↓</td>
<td>↑</td>
<td>↑↑↑</td>
<td>+</td>
<td>↑</td>
<td>↓↓</td>
<td>↑</td>
<td>↓↓</td>
<td>↑↑↑</td>
</tr>
<tr>
<td>E-commerce segment</td>
<td>↑</td>
<td>↑↑↑</td>
<td>↑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>↑</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>Content segment</td>
<td>↓↓↓</td>
<td>↓↓↓</td>
<td>↓</td>
<td>↓</td>
<td>↓</td>
<td>↓</td>
<td>↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>←</td>
</tr>
<tr>
<td>Premium accounts offered</td>
<td>↑↑↑</td>
<td>↑↑↑</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>↑</td>
<td>←</td>
<td>↑↑↑</td>
<td>↓↓</td>
<td>←</td>
</tr>
<tr>
<td>Payment details stored</td>
<td>↑↑↑</td>
<td>↑↑↑</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>↑</td>
<td>←</td>
<td>↑↑↑</td>
<td>↓↓</td>
<td>←</td>
</tr>
<tr>
<td>E-mail provided</td>
<td>+</td>
<td>↓↓↓</td>
<td>↑↑</td>
<td>←</td>
<td>↑</td>
<td>↑↑</td>
<td>←</td>
<td>←</td>
<td>↑↑↑</td>
<td>↑↑↑</td>
</tr>
<tr>
<td>Social networking features</td>
<td>+</td>
<td>↓↓↓</td>
<td>↑↑</td>
<td>←</td>
<td>↑</td>
<td>↓</td>
<td>↑↑↑</td>
<td>↑↑↑</td>
<td>↑↑</td>
<td>↑↑</td>
</tr>
</tbody>
</table>
Security policies vary far more than requirements

No TLS, no password requirements, cleartext passwords emailed, no guessing or user probing restrictions, email addresses verified

No TLS, no password requirements or advice, emailed temp. passwords for reset, no password advice, no guessing or user probing restrictions, email addresses verified

TLS deployed, 6 char. min. password, emailed reset links, no password advice, guessing restrictions in place, email addresses verified

No TLS, 6 char. min. password, personal knowledge questions for reset, no password advice, no guessing or user probing restrictions, email addresses verified

TLS deployed, 6 char. min. password, emailed reset links, no password advice, guessing restrictions in place, email addresses verified

---

J. Bonneau, S. Preibusch (U. of Cambridge)  The password thicket  June 7, 2010  22 / 28
Findings

1. How does the user experience vary from site to site?
2. What implementation weaknesses exist?
3. Which circumstantial factors affect sites’ implementation choices?
4. How do sites’ security requirements affect their choices?
5. Why do websites choose to collect passwords?
### Tell Us About Yourself (Required)

- **Gender:** Male, Female
- **Year of Birth:** 1972 (Click here if you are under 13)
- **ZIP Code:** 12345
- **Country of Residence:** United States
- **Household Income:** $150,000 or more
- **Job Title:** CEO/President/Chairman
- **Industry:** Manufacturing
- **Company Size:** 1000+

New York Times
### Content sites want email, marketing data

<table>
<thead>
<tr>
<th>Data</th>
<th>I</th>
<th>E</th>
<th>C</th>
<th>Tot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>38</td>
<td>50</td>
<td>49</td>
<td>137</td>
</tr>
<tr>
<td>Email verified</td>
<td>29</td>
<td>1</td>
<td>35</td>
<td>65</td>
</tr>
<tr>
<td>Email updates offered</td>
<td>21</td>
<td>42</td>
<td>47</td>
<td>110</td>
</tr>
<tr>
<td>Postcode</td>
<td>15</td>
<td>30</td>
<td>34</td>
<td>79</td>
</tr>
<tr>
<td>Mailing address</td>
<td>5</td>
<td>19</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>Phone number</td>
<td>5</td>
<td>20</td>
<td>7</td>
<td>32</td>
</tr>
<tr>
<td>Marketing data</td>
<td>4</td>
<td>6</td>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>Username</td>
<td>35</td>
<td>5</td>
<td>29</td>
<td>69</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>29</td>
<td>3</td>
<td>11</td>
<td>43</td>
</tr>
</tbody>
</table>
Password over-collection is a tragedy of the commons
Password insecurity is a negative externality
Economic models

- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality
Economic models

- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality
Regulatory fixes

- Tax
- Licensing
- Liability
- Standards
**Regulatory fixes**

- **Tax**
- **Licensing**
- **Liability**
- **Standards**
Regulatory fixes

- Tax
- Licensing
- Liability
- Standards
Regulatory fixes

- Tax
- Licensing
- Liability
- Standards
Regulatory fixes

- Tax
- Licensing
- Liability
- Standards
It’s a thicket out there

- The market is failing
- Psychological barriers may exist
Perspectives

- It’s a thicket out there
- The market is failing
- Psychological barriers may exist
It’s a thicket out there
The market is failing
Psychological barriers may exist
Registering for Mixx is fast, fun, and easy! Here at Mixx, we don't think you should have to create yet another username and password. We work with several sites that you may already use. Simply select the account you'd like your new Mixx account to work with and we'll handle the rest!

Register using your OpenID URL

Mixx
Feeling geeky?

When you log in to a website that supports OpenID login we’ll send your OpenID identifier to the website so it can identify you.

To make things easy, we have generated this identifier for you: https://me.yahoo.com/a/OU2iCjRytdHt3TZVle

You don't need to save this identifier. While logging in to websites, you can simply look for a Yahoo! button or type yahoo.com in the OpenID text field. You can also choose additional custom identifiers for your Yahoo! account below.

Yahoo!
Questions?

jcb82@cl.cam.ac.uk
sdp36@cl.cam.ac.uk

Data available online:
http://preibusch.de/publ/password-market