technical and market failures in human authentication on the web

By:
Joseph Bonneau
Sören Preibusch

Reviewed by:
Komal Sachdeva
MT10007
Some Definitions:

PASSWORD:  
A secret word or phrase known only to a restricted group.

THICKET:  
A dense growth of shrubs or underbrush.
Recent Examples

Twitter hack.

2009

http://en.webrazzi.com/
Motivation and Related Work.

HUMAN ASPECT

Easily guessable passwords.

- password cracking
- Writing down.
- social engineering attack
- Reuse.

the average web user was found to maintain 25 separate password accounts, with just 6.5
Motivation and Related Work.

HUMAN ASPECT

Sharing password.

- sharing password increases intimacy between couples.
- teenagers share them casually.
Motivation and Related Work.

INDUSTRY ASPECT

Improved storage
  salted and hashed password
Password entry.
  cued recall system
  mnemonic password
  graphic password
Motivation and Related Work.

Single sign on system.

- OpenID
- Facebook Connect
- Password Standardization
- ISO27001
- TLS implementation

Falk et al.’s study were that most banking websites (76%) suffered at least one noticeable design flaw of the 5 checked for, including 30% of banks failing to use TLS.
Selection of sites.

Their study included 150 websites which offer free user accounts for a variety of purposes, including the most popular destinations on the web and a random sample of e-commerce, news, and communication websites.
Work Done.

<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>
Evaluation Basis.

Enrollment.

strong password, requesting email

Login/Logout.

password transmitted safely?

Password Updates

length and content of the password
Analysis

Varied User Experience

advice for password protection.

78% of sites provided no advice or guidance on what a password is, demonstrating that users are expected to have internalised the concept of webbased password login.
Analysis

varied amount of data collected

<table>
<thead>
<tr>
<th>Data</th>
<th>Identity</th>
<th>E-Commerce</th>
<th>Content</th>
<th>Total</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 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>Username</td>
<td>35</td>
<td>5</td>
<td>29</td>
<td>69</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>CAPTCHA</td>
<td>29</td>
<td>3</td>
<td>11</td>
<td>43</td>
</tr>
</tbody>
</table>
Analysis

Security weakness

Lack of standardization

Password recovery

• Email based – 48%
• Temporary password - 27%
• Cleartext password – 25%
Analysis

Lack of standardization: Password length

http://preibusch.de/publ/password-market
Security weakness

Password guessing

Time out- only permitted to make 4 login attempts a minute.

CAPTCHA
Clusters of websites

http://preibusch.de/publ/password-market
### Site’s security implementation

<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>

[http://preibusch.de/publ/password-market]
Analysis

Most popular deploy better password security

http://preibusch.de/publ/password-market
Analysis

Site’s security requirement

Content sites require less rigorous password security measures than e-commerce websites.

Payment sites were also more
Analysis

Password collection

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

http://preibusch.de/publ/password-market
Economic model

Password security as a tragedy of common.

To prevent depletion of their password memory, consumers must either reduce the burden for each individual password by choosing weaker passwords or reduce the cumulative burden by re-using passwords.

Password insecurity as a negative externality.

Web sites with poor password security impose a strong negative externality on sites which have implemented more security, as they
Proposed Solution

Password Tax.
Restricting password re-use by password segmentation
Liability
Technical standards
Thank you...