Application Security and User Experience

Alex Smolen
OWASP AppSec USA 2011
Lost iPod Touch
$50 Reward
Call Caroline MacLure
443-629-

Lost iPod Touch
$50 reward
Call
410-859-
SECURITY
They'll Never Figure Out Your Combination
### My Top-SECRET Passwords

<table>
<thead>
<tr>
<th>Title</th>
<th>URL</th>
<th>Start Date</th>
<th>Exp. Date</th>
<th>Status</th>
<th>Membership</th>
<th>Shared</th>
<th>Paid</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hospital</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>College</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Home</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Why try to remember what you could just write down!*
The more secure you make something, the less secure it becomes.

Don Norman
Dylan: wow! you can type your facebook password into a comment and it comes up as stars!! ********** hahaha thats so cool!

4 hours ago

Übermensch: ********** Holy shit, you're right.

3 hours ago

Edizzle: **********

2 hours ago

Edizzle: Too cool

2 hours ago

Luke: isecretlylove50cent

about an hour ago

Luke: FUCK I FUCKING HATE YOU

about an hour ago
Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
\[ H = L \frac{\log N}{\log 2} \]

where \( N \) is the number of possible symbols and \( L \) is the number of symbols in the password.
We conclude that forcing users to choose strong passwords appears misguided: this offers no defense against the common password stealing attacks and there are better means to address bulk guessing attacks.

Logon Message

Your password has expired and must be changed.
Hi

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/settings/resetpassword/?id=5811756&key=

Thanks,
The Last.fm Team

Change your Last.fm email settings here: http://www.last.fm/settings/notifications

Or to directly unsubscribe from all emails without any nonsense: http://www.last.fm/settings/unsubscribe/?auth=8234945811756

Last.fm Ltd, Karen House, 1–11 Baches Street, London, UK, N1 6DL
Because of inactivity, your session has timed out and is no longer active. Click OK to reload the page.
KEEP ME LOGGED IN CHECK

Y U NO KEEP ME LOGGED IN
A continually improving collection of questions and answers created, edited, and organized by everyone who uses it.

You are now logged out of your account in this browser, but you are still logged in from 1 other browser.

Login to Quora or Create an Account

Alex
Login As Another User
I Can Relate:
"Username or Password is Incorrect."...why don't you just tell me which one?!
Security Information
This page contains both secure and nonsecure items.
Do you want to display the nonsecure items?

Yes  No  More Info

Internet Explorer
This page has an unspecified potential security risk.
Would you like to continue?

Yes  No
There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

- Click here to close this webpage.
- Continue to this website (not recommended).
- More Information
Emperor’s New Security Indicators

- 57 subjects
- How many withheld password?
  - 0 after HTTPS removed
  - 2 after site authentication image removed
  - 25 after warning page
  - 30 always typed in their password

Source: http://usablesecurity.org/emperor/
Johnny can’t encrypt

- 12 subjects using PGP
- How many sent secure email?
  - 3 emailed the private key
  - 1 forgot the passphrase
  - 7 used their public key to encrypt
  - Only 2 of 5 encrypted messages were decrypted

Source: http://usenix.org/events/sec99/whitten.html
Security Check

Enter both words below, separated by a space.
Can't read the words below? Try different words or an audio captcha.

Text in the box:

infinite beer

Submit  Cancel
HOW SECURE IS MY PASSWORD?

Common Password: In The Top 40 Most Used Passwords
Your password is very commonly used. It would be hacked almost instantly.

Possibly A Word
Your password looks like it could be a dictionary word or a name. If it's a name with personal significance it might be easy to guess. If it's a dictionary word it could be hacked very quickly.

Length: Very Short
Your password is very short. The longer a password is the more secure it will be.

Character Variety: Just Letters
Your password only contains letters. Adding numbers and symbols can make your password more secure.
Warning: Suspected phishing site!

The website at static.ak.fbcdn.net has been reported as a "phishing" site. Phishing sites trick users into disclosing personal or financial information, often by pretending to represent trusted institutions, such as banks.

Learn more about phishing scams.

[Buttons: Proceed anyway, Back to safety]

Report an error
Warning: We believe your account was recently accessed from: Poland

Your filters are forwarding some of your email to 2 other email addresses
Continue to Books?

You are allowing Books access to both you and your friends information below:

Others Have Allowed

- Name: Andrew Besmer
- * Networks: UNC Charlotte
- * Movies: WALL-E 16%
- Books: The Cat in the 92%

Also give Books the following information about your friends:

- Name: Heather Richter Lipford, etc...
- Networks: UNC Charlotte
- Movies: Ratatouille
- Books: Green-Eggs and Ham

Continue to... or Cancel
Request for Permission

Cool Social App is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Send me email
Cool Social App may email me directly at brent@example.com - Change

Access my profile information
Birthday

Report Application

Logged in as [redacted] (Not You?)

[Allow] [Don’t Allow]
<table>
<thead>
<tr>
<th>Browser</th>
<th>Standard SSL</th>
<th>EVSSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 9</td>
<td>Gray padlock in address bar</td>
<td>Gray padlock plus full green address bar with company name or CA</td>
</tr>
<tr>
<td>Internet Explorer 8</td>
<td>Yellow padlock in address bar</td>
<td>Yellow padlock plus full green address bar with company name or CA</td>
</tr>
<tr>
<td>Firefox 4</td>
<td>Blue security emblem in address bar</td>
<td>Green security emblem in address bar with company name</td>
</tr>
<tr>
<td>Firefox 3</td>
<td>Padlock at bottom plus blue security emblem in address bar</td>
<td>Padlock at bottom plus green emblem in address bar with company name</td>
</tr>
<tr>
<td>Chrome 11</td>
<td>Green padlock in address bar</td>
<td>Green padlock plus green emblem in address bar with company name</td>
</tr>
<tr>
<td>Opera 11</td>
<td>Dark padlock plus yellow emblem in address bar written as “Secure”</td>
<td>Dark padlock plus green emblem in address bar written as “Trusted”</td>
</tr>
<tr>
<td>Konqueror 4</td>
<td>Green shield with white check mark in address bar</td>
<td>Green shield with white check mark in address bar</td>
</tr>
<tr>
<td>Safari 5</td>
<td>Gray padlock in address bar</td>
<td>Gray padlock plus green company name in address bar</td>
</tr>
</tbody>
</table>

Source: http://www.lookout.net/?p=530
Figure 1: The trusted password window uses a background image to prevent spoofing of the window and textboxes.

Source: http://www.ischool.berkeley.edu/research/publications/tygar/2007/dynamic
## The Acme Policy

<table>
<thead>
<tr>
<th>types of information</th>
<th>how we use your information</th>
<th>who we share your information with</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>provide service &amp; maintain site</td>
<td>research &amp; development</td>
</tr>
<tr>
<td>contact information</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>cookies</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>demographic information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>financial information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>health information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>preferences</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>purchasing information</td>
<td>!</td>
<td>!</td>
</tr>
</tbody>
</table>

Source: [http://cups.cs.cmu.edu/privacylabel/](http://cups.cs.cmu.edu/privacylabel/)
The application's digital signature has been verified.
Do you want to run the application?

Name: [redacted]
Publisher: [redacted]
From: [redacted]

Always trust content from this publisher.

Run  Cancel

The digital signature has been validated by a trusted source.
More Information...
This application has access to the following:

⚠️ **Your location**
- coarse (network-based) location, fine (GPS) location

⚠️ **Default**
- Read Google service configuration

⚠️ **Network communication**
- full Internet access

⚠️ **Your accounts**
- Google Docs, Google Maps, Google Spreadsheets, manage the accounts list, use the authentication credentials of an account

⚠️ **System tools**
- prevent phone from sleeping
Balance
Too much security can be counter-productive
Usability for us