

User authentication on the web

Joseph Bonneau

jcb82@cl.cam.ac.uk



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory

SOCIALNETS workshop
November 18, 2010

Looming authentication challenges

- 1 The old world
- 2 The emerging world

WEIS 2010: Large study of password deployments



[View Photos of Me \(533\)](#)
[View Videos of Me \(2\)](#)
[Edit My Profile](#)

[Write something about yourself.](#)

Information


Networks:
Cambridge Grad Student '11
Stanford Alum '06


Birthday:
July 17, 1984

Current City:
San Francisco, CA

Friends

664 friends [See All](#)


Brett Talbot Ryan Sili Tyler Jank


Chris Ching Bob Borek Katie Stenson

Joseph Bonneau

[Wall](#) [Info](#) [Photos](#) [Boxes](#) [+](#)

What's on your mind?

Attach:     [Share](#)

[Options](#)

Molly Fox
In these photos: Joseph Bonneau



Hail the MiniCleggs of Bratislava
Easter, part the first.
May 23 at 7:07pm - [View album](#)

Stella Nordhagen
In these photos: Joseph Bonneau



Holi Holi Holi
9 new photos
A (belated) celebration of colour!
May 18 at 4:53pm - [View album](#)

RECENT ACTIVITY

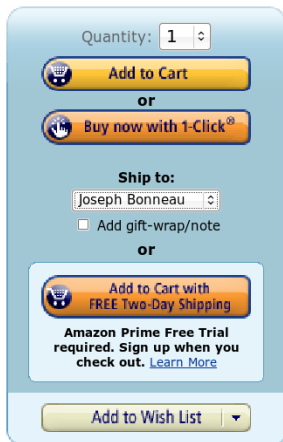
 Joseph is now friends with Michelle Russo Vinroe and Katie Haberman.

 Joseph attended Gates Distinguished Lecture. - [Comment](#) - [Like](#)


 Joseph and Noah Isserman are now friends. - [Comment](#) - [Like](#)

“Identity” websites


WEIS 2010: Large study of password deployments



Quantity:

 **Add to Cart**


or

 **Buy now with 1-Click[®]**

Ship to:

☐ Add gift-wrap/note

or


 **Add to Cart with
FREE Two-Day Shipping**

**Amazon Prime Free Trial
required. Sign up when you
check out. [Learn More](#)**


Add to Wish List ▼

“E-Commerce” websites


WEIS 2010: Large study of password deployments

 CURRENT E-MAILS


You have no subscriptions for Email newsletters.

 MY ALERTS [+ Create News Alert](#)

You have no alerts, use the "Create News Alert" link above to create one.

 MY STOCK ALERTS [+ Create Stock Alert](#)

You have no alerts, use the "Create Stock Alert" link above to create one.

 COMMENT NOTIFICATIONS

Receive a notification when your comment is posted or replied to by an NYTimes reporter. [SUBSCRIBE](#)

TODAY'S HEADLINES

TODAY'S HEADLINES [SUBSCRIBE](#)

DAILY

Get general top headlines or create a customized e-mail by selecting from the categories below.

[See Sample](#)

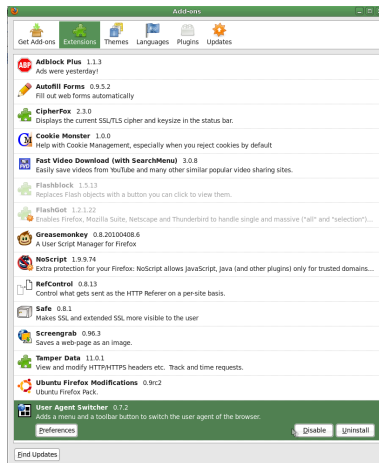
<input type="checkbox"/> U.S	<input type="checkbox"/> Daily Featured Section	<input type="checkbox"/> Editorial
<input type="checkbox"/> Sports	<input type="checkbox"/> Business	<input type="checkbox"/> Technology
<input type="checkbox"/> Politics	<input type="checkbox"/> World	<input type="checkbox"/> NY Region
<input type="checkbox"/> Op-Ed	<input type="checkbox"/> Arts	

“Content” websites

WEIS 2010: Large study of password deployments

Mozilla Firefox v 3.5.8 with:

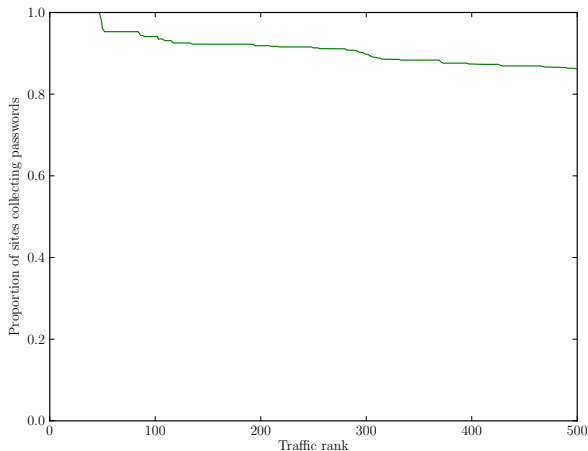
- **Autofill Forms 0.9.5.2**
- **CipherFox 2.3.0**
- **Cookie Monster 0.98.0**
- **DOM Inspector 2.0.4**
- **Greasemonkey 0.8.20100211.5**
- **Screengrab 0.96.2**
- **Tamper Data 11.0.1**



WEIS 2010: Large study of password deployments

feature	scoring
enrolment	
Password selection advice given	+1 pt
Minimum password length required	+1 pt
Dictionary words prohibited	+1 pt
Numbers or symbols required	+1 pt
User list protected from probing	+1 pt
Cleartext password sent in email after enrolment	-1 pt
login	
Password hashed in-browser before POST	+1 pt
Limits placed on password guessing	+1 pt
User list protected from probing	+1 pt
Federated identity login accepted	+1 pt
password update	
Password re-entry required to authorise update	+1 pt
Notification email sent after password reset	+1 pt
password recovery	
Password update required after recovery	+1 pt
Cleartext password sent in email upon request	-1 pt
User list protected from probing	+1 pt
encryption	
Full TLS for all password submission	+2 pts
POST only TLS for password submission	+1 pt

The realities of web authentication



Frequency of password collection

The realities of web authentication

- ~ all websites collect email address as username
- ~ all websites use email for password reset
- ~ all websites use persistent login cookies by default

Many schoolbook errors are quite common

Change Your Password (optional)

A Password must be at least 6 characters or longer, and may not include blank spaces, or the characters: <> " (A good example of a password: *RUGT_7*).

New Password: Please note passwords are case sensitive.

Confirm Password:

29-50% of sites store passwords in the clear

Many schoolbook errors are quite common

guardian.co.uk Search

[News](#) [Sport](#) [Comment](#) [Culture](#) [Business](#) [Money](#) [Life & style](#) [Travel](#) [Environment](#)

[News](#) [Technology](#) [Technology blog](#)

TECHNOLOGY BLOG



[Previous](#) [Blog home](#) [Next](#)

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



Part of the RockYou website

Posted by Jack Schofield Tuesday 15 December 2009 17:33 GMT [guardian.co.uk](#)

[larger](#) [smaller](#)

Technology
Hacking · Data and computer security · Cloud computing

Media
Social networking

[More from Technology blog on](#)

RockYou SQL injection hack January 2010

Many schoolbook errors are quite common

countermeasure	I	E	C	Tot.
CAPTCHA	11	2	1	14
timeout	2	1	2	5
reset	1	3	1	5
none	37	43	46	126

Many websites allow unlimited brute-force guessing

Many schoolbook errors are quite common

Sign In

E-mail:

Password:

☒ Remember me on this computer

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

Sign In

[Forgot your password?](#)

Ask

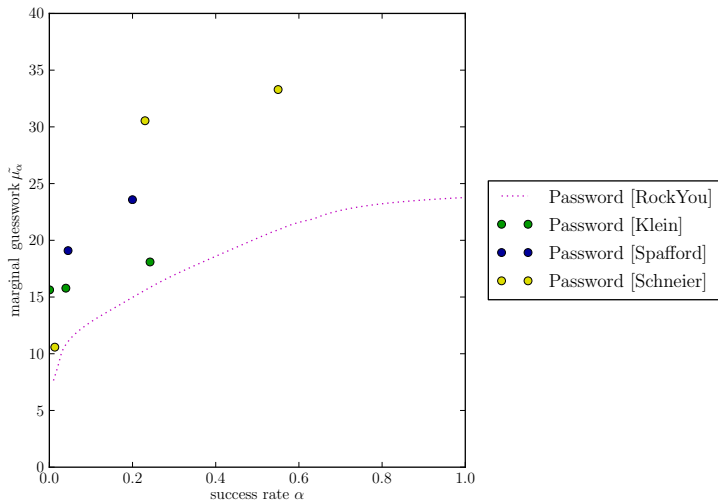
User probing is rarely prevented

Many schoolbook errors are quite common

interface	I	E	C	Tot.
enrolment	4	1	1	6
login	43	41	38	132
reset	11	7	2	20
all	1	1	0	2

User probing is rarely prevented

Many schoolbook errors are quite common



Many schoolbook errors are quite common

TLS Deployment	I	E	C	Tot.
Full	10	39	10	59
Full/POST	3	1	1	5
Inconsistent	14	6	5	25
None	23	4	34	61

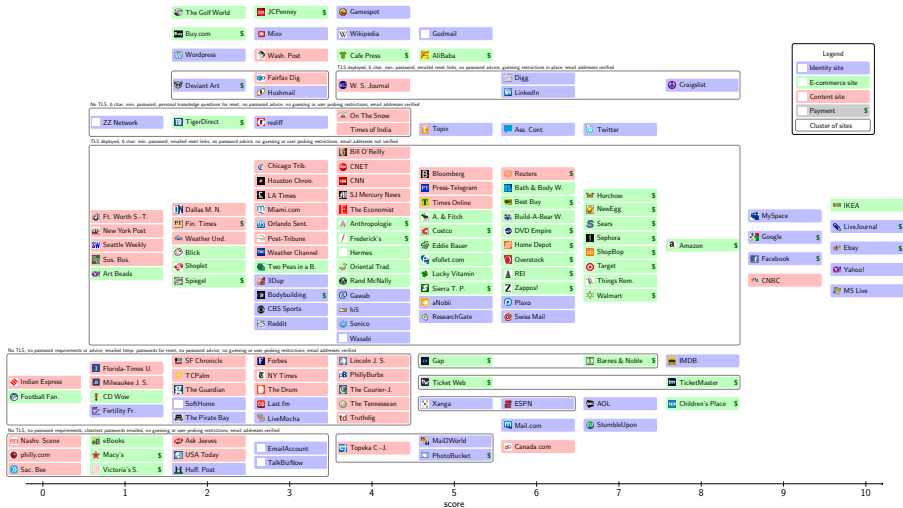
TLS deployment remains uneven, poorly done

Many schoolbook errors are quite common

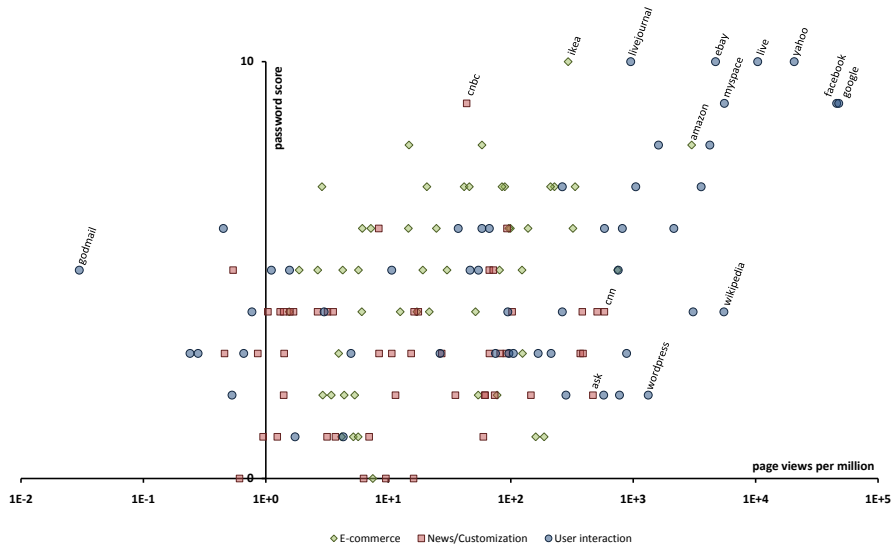
The screenshot shows a web browser window with multiple tabs open, including 'Firesheep', 'twitter - Goo...', 'Gmail - [Meet...]', '(119) Twitter ...', 'Top 150 Soci...', 'Hotmail - lwa...', and 'Facebook (3)'. The main content is the Facebook News Feed for the user 'Mike Mcallen'. The sidebar on the left lists contacts: Mike Mcallen (Facebook), meetingspodcast@gmail.com (Google), mmcallen (Twitter), and several instances of 'Alice, or perhaps Bob' (Windows Live) and 'Larry Walters' (Facebook). The News Feed includes a post from 'November USA' about a photo contest, a video post from 'David Spark' about recruiting practices, a post from 'Melissa Kane' about Steve Miller, and a post from 'Marianne Mattson' about a drunk rant. The right sidebar features sections for 'Events', 'People You May Know' (listing Aaron McDougall and Dennis Hamilton), 'Sponsored' (Booming Business Tips), and 'Requests'.

Firesheep

Security policies vary far more than requirements



More popular sites do better



Twitter accounts compromised in torrent site scam

Angela Moscaritolo February 03, 2010



PRINT



EMAIL



REPRINT



PERMISSIONS

FONT SIZE: A | A | A



Tweet

0



Like

Twitter this week reset the passwords of some of its users after discovering malicious file-sharing sites that were set up to steal users' login credentials.

During regular monitoring of its user base for suspicious activity, Twitter noticed a sudden surge in followers for several accounts within the last five days, Del Harvey, Twitter's director of trust and safety, wrote in a [blog post](#) Tuesday. After investigating the issue, Twitter discovered that some of the accounts following the suspicious users were compromised by an attacker who stole login credentials from rogue [file-sharing](#) "torrent" sites.

For several years, an individual had been setting up torrent sites, as well as forums for torrent site usage, Harvey said. This individual sold these supposedly well-crafted sites and forums to others who wanted to start their own torrent download sites.

RELATED ARTICLES

- [Twitter hackers compromise Chinese search engine](#)
- [Twitter attributes outage to DNS records hack](#)
- [SSL bug used on Twitter](#)
- [Spears Twitter hack](#)
- [New Twitter worm strikes](#)
- [Twitter among web apps affected by patched XSS bug](#)
- [Twitter XSS vulnerability not yet fixed](#)
- [Twitter fights off massive DoS attack](#)
- [Researchers laud Twitter alerts on bad links](#)
- [Koobface hits Twitter](#)

RELATED LINKS

- [Twitter](#)

- Bad websites can do real damage to good ones
- Password insecurity is a negative externality
- Password over-collection is a tragedy of the commons

Economic failures



- Bad websites can do real damage to good ones
- Password insecurity is a negative externality
- Password over-collection is a tragedy of the commons

Economic failures



- Bad websites can do real damage to good ones
- Password insecurity is a negative externality
- Password over-collection is a tragedy of the commons

Looming authentication challenges

- 1 The old world
- 2 The emerging world

OpenID—Single sign-on

- R** Relying party (www.example.com)
- P** OpenID Provider (Facebook, Google, etc.)
- U_E** End user (a human)
- U_A** User agent (a browser)

U_E → **R** I'm **U@P**!

OpenID—Single sign-on

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

Register



OpenID—Single sign-on

- R** Relying party (www.example.com)
- P** OpenID Provider (Facebook, Google, etc.)
- U_E** End user (a human)
- U_A** User agent (a browser)

U_E \longrightarrow **R** I'm **U**@**P**!

R \longleftrightarrow **P** $K_{R-P}, n \leftarrow$ D-H key exchange

OpenID—Single sign-on

- R** Relying party (www.example.com)
- P** OpenID Provider (Facebook, Google, etc.)
- U_E** End user (a human)
- U_A** User agent (a browser)

- U_E** → **R** I'm **U@P**!
- R** ↔ **P** $K_{R-P}, n \leftarrow$ D-H key exchange
- U_E** ← **R** OK, go verify with **P** (HTTP 302)
- U_E** → **P** I want to talk to **R**, who you share n with

OpenID—Single sign-on

- R** Relying party (www.example.com)
P OpenID Provider (Facebook, Google, etc.)
U_E End user (a human)
U_A User agent (a browser)

- U_E** \longrightarrow **R** I'm **U@P**!
R \longleftrightarrow **P** $K_{R-P}, n \leftarrow$ D-H key exchange
U_E \longleftarrow **R** OK, go verify with **P** (HTTP 302)
U_E \longrightarrow **P** I want to talk to **R**, who you share n with
U_E \longleftarrow **P** Sure you want to talk to **R**?

OpenID—Single sign-on



[Sign in as a different user](#)

You are signing in to **Mixx.com** with your Google Account **jbonneau@gmail.com**

Sign in

Cancel

☒ Remember me

You can always change your Google Account approval settings. Mixx.com is not owned, operated or controlled by Google or its owners. [Learn more](#)

OpenID

OpenID—Single sign-on

- R** Relying party (www.example.com)
P OpenID Provider (Facebook, Google, etc.)
U_E End user (a human)
U_A User agent (a browser)

- U_E** → **R** I'm **U@P**!
R ↔ **P** $K_{R-P}, n \leftarrow$ D-H key exchange
U_E ← **R** OK, go verify with **P** (HTTP 302)
U_E → **P** I want to talk to **R**, who you share n with
U_E ← **P** Sure you want to talk to **R**?
U_E → **P** Yes, here's my password: p

OpenID—Single sign-on

R Relying party (www.example.com)
P OpenID Provider (Facebook, Google, etc.)
U_E End user (a human)
U_A User agent (a browser)

U_E → **R** I'm **U@P**!
R ↔ **P** $K_{R-P}, n \leftarrow$ D-H key exchange
U_E ← **R** OK, go verify with **P** (HTTP 302)
U_E → **P** I want to talk to **R**, who you share n with
U_E ← **P** Sure you want to talk to **R**?
U_E → **P** Yes, here's my password: p
U_E ← **P** Okay, use **MAC** $_{K_{R-P}}(\mathbf{U}, \mathbf{P})$ (HTTP 302)
U_E → **R** **MAC** $_{K_{R-P}}(\mathbf{U}, \mathbf{P})$! See, I'm **U@P**

OpenID—Single sign-on

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!

OpenID—Single sign-on

- R** Relying party (www.example.com)
P OpenID Provider (Facebook, Google, etc.)
U_E End user (a human)
U_A User agent (a browser)

U_E → **R** I'm **U@P**!
R ↔ **P** $K_{R-P}, n \leftarrow$ D-H key exchange
U_A ← **R** OK, go verify with **P** (HTTP 302)
U_A → **P** I want to talk to **R**, here's my cookie c
U_A ← **P** Okay, use $\text{MAC}_{K_{R-P}}(\mathbf{U}, \mathbf{P})$
U_A → **R** $\text{MAC}_{K_{R-P}}(\mathbf{U}, \mathbf{P})!$ See, I'm **U@P**

(auth-immediate)

The Dark Ages

Find people you know on Facebook

Your friends on Facebook are the same friends, acquaintances and family members that you communicate with in the real world. You can use any of the tools on this page to find more friends.



Find People You Email

[Upload Contact File](#)

Searching your email account is the fastest way to find your friends on Facebook.

Your Email:

Email Password:

[Find Friends](#)

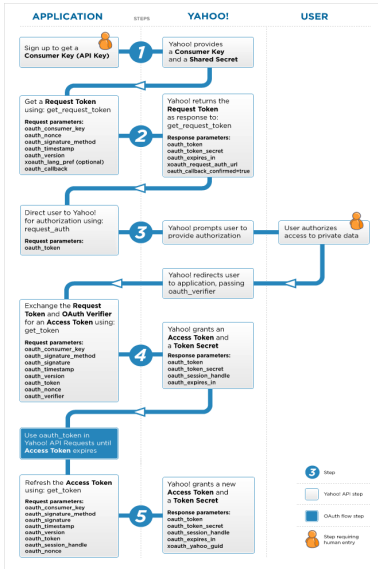


Facebook will not store your password. [Learn More.](#)

The Middle Ages

- 1 Facebook Connect
- 2 Google AuthSub
- 3 Yahoo BBAuth
- 4 Twitter API: HTTP basic-authentication

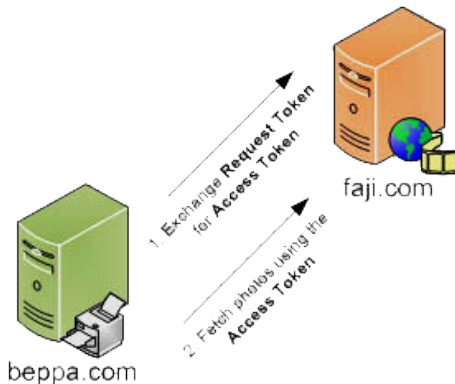
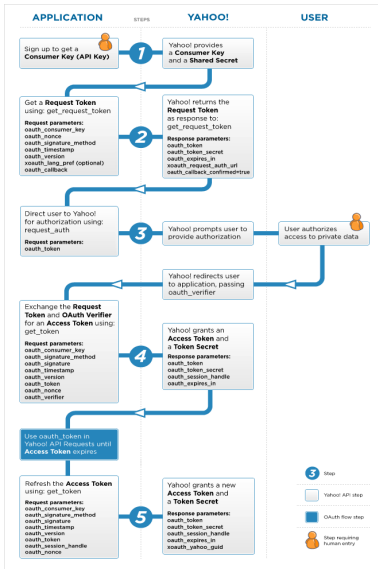
OAuth—Delegating API access



Basic Information		
Application Name	<input type="text" value="Test"/>	Cannot contain Facebook trademarks
Description	<input type="text"/>	The plaintext description of your application
Icon	<input type="text" value="Change your icon"/>	Appears next to your application name throughout Facebook (1x16)
Logo	<input type="text" value="Change your logo"/>	Appears in authentication dialogs, search results, and the app directory (75x75)
Language	<input type="text" value="English (US)"/>	The native language of your application
User Support Address	<input type="text" value="Email: jbonneau@gmail.com"/>	The email address or URL where users can contact you about your application
Contact Email	<input type="text" value="jbonneau@gmail.com"/>	The email address where Facebook can contact you or your company
Privacy Policy URL	<input type="text"/>	The URL to your application's privacy policy, required for the permissions dialog
Terms of Service URL	<input type="text"/>	The URL to your application's terms of service, used in the permissions dialog
Developers		
Developers	<input type="text" value="Joseph Bonneau Remove"/>	Developers can edit this application and may appear on the application profile
Add Developers	<input type="text" value="Start typing a friend's name"/>	Developers added here will be sent a request and shown as "pending" until they accept the request

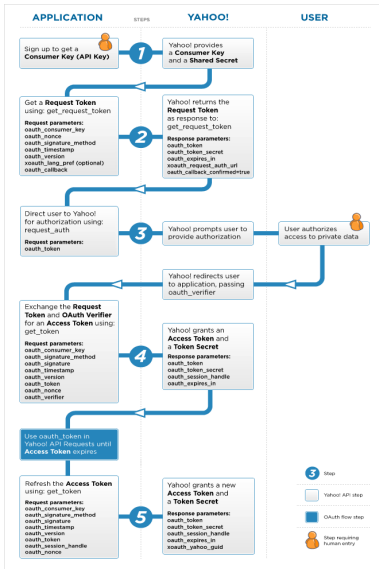
- 1 App registration
- 2 Access request
- 3 User approval
- 4 API Access

OAuth—Delegating API access



- 1 App registration
- 2 Access request
- 3 User approval
- 4 API Access

OAuth—Delegating API access



Request for Permission

FarmVille 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.



Access my profile information
Birthday and Current City

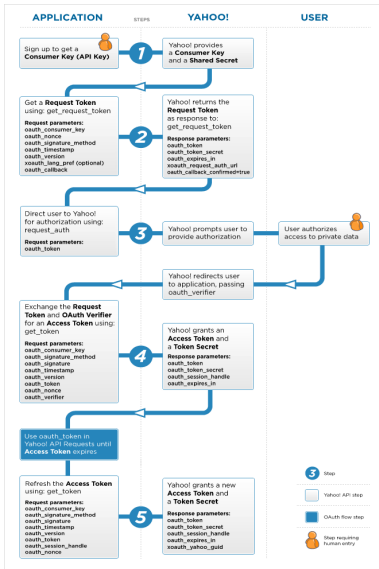
By proceeding, you agree to the FarmVille Terms of Service and Privacy Policy · Report Application

Logged in as (Not You?)

Allow **Leave Application**

- 1 App registration
- 2 Access request
- 3 User approval
- 4 API Access

OAuth—Delegating API access



PLAINTEXT:
 $M || K_{app} || K_{user}$

HMAC_SHA1:
 $MAC_{K_{app} || K_{user}}(M)$

RSA_SHA1:
 $Sign_{K_{app}}(M)$

- 1 App registration
- 2 Access request
- 3 User approval
- 4 API Access

Open issues

- 1 Standardisation
- 2 Branding
- 3 Security level
- 4 Service discovery

Interaction via iframe

Slate

NOV. 18, 2010

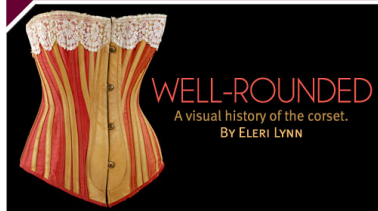
BRIEFING NEWS & POLITICS ARTS LIFE BUSINESS & TECH SCIENCE PODCASTS & VIDEO BLOGS

Search

Why Do Auctioneers Talk Like That?



Slate bing



The Slatest

1. AP: Murkowski Wins Alaska Race
2. Pelosi Wins Leadership Re-Election
3. GOP Puts Obama's Russia Treaty on Ice
4. First Cholera Case Reported in U.S.

....>

TODAY'S PICTURES

TODAY'S CARTOONS

TODAY'S DOONESBURY

TODAY'S VIDEO

Fortresses.



Tax Relief NOW
Everything You Need To Know About the Congressional Fight Over the Bush Tax Cuts



Six Smart Compromises Pro-Choice Activists Can Make In the Abortion Debate



The Best Movie Cameos by Politicians



My Friend and I Have Tickle Fights All the Time. I Think I'm Falling in Love With Her.

BRIEFINGS

Explainer

The Slatest

Today's Pictures

TODAY IN SLATE

SLATE BLOGS

Wednesday, Nov. 17, 2010

Slate Slate.com on Facebook



Caitlin M Casey shared Democrats didn't lose the battle of 2010. They won it. · about a week ago



Eli Davidson liked Democrats didn't lose the battle of 2010. They won it. · about a week ago



Jerry Cain shared What should you do if you're attacked by a mountain goat? · about a month ago



Garth Strohbehn shared Should you crowdsourc your medical problems? · about a month ago

View My Network on Slate >>

Preventing surrepititious authentication

```
<img id="test" style="display:none">

<script>
test = document.getElementById('test');
var start = new Date();
test.onerror = function()
{ time = new Date() - start;}

test.src = "http://www.example.com/";
</script>
```

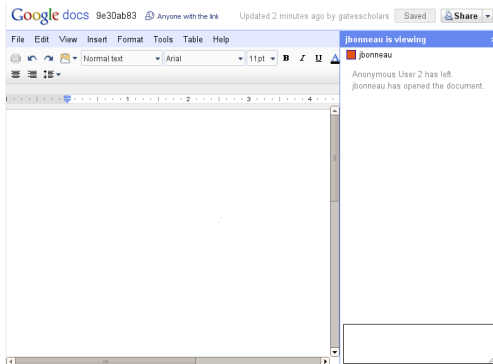
Bortz et al. 2007

Preventing surreptitious authentication

```
# Send users to my detector...  
<iframe name="detector"  
width="0" height="0" frameborder="0"  
src="https://docs.google.com/document/d/  
1TUV9x1lFAQcVWvhP4EAHQZlPrVmo3_vrz5Sz8Wo">  
</iframe>
```

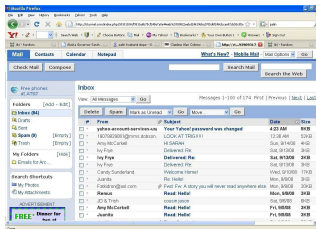
Narayanan 2009

Preventing surreptitious authentication



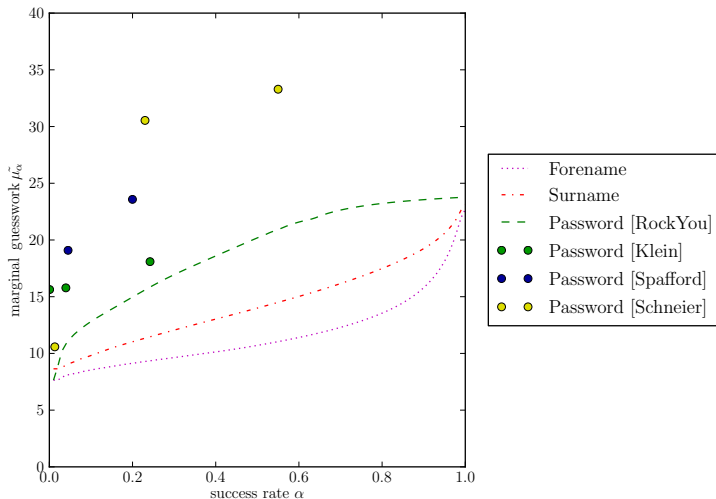
Narayanan 2009

Workable backup authentication



- Web search
 - Reaching a head with OSNs
- Public records
 - Griffith et. al: 30% of individual's mother's maiden names
- Social engineering
- Dumpster diving, burglary
- Acquaintance attacks
 - Schechter et. al: ~ 25% of questions guessed by friends, family

Workable backup authentication



Personal knowledge worse than passwords (Bonneau et al. 2010)

Workable backup authentication



Recovering your password

Add more information to your account to increase your account-recovery options.

Email

Receive a password-reset link at an email address which you can access.

[Add an email address.](#)

SMS

Receive a text message with a password-reset code on your mobile phone.

Country

United Kingdom

Mobile phone number

+44 07590 677117

Security question

Answer a question to reset your password.

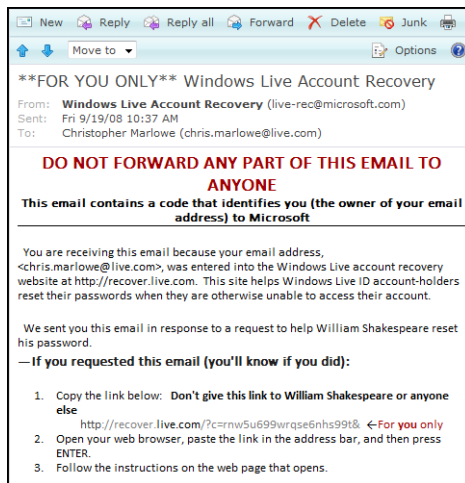
[Edit](#)

Save

Cancel

Google—backup authentication by mobile phone

Workable backup authentication



Schecter et al. 2008

MS Live (proposed)—social backup authentication

Workable backup authentication

The screenshot shows a web browser window titled "Windows Live ID Account Recovery - Windows Internet Explorer". The address bar shows "http://recover.live.com/". The page content includes a heading "Help a friend reset his or her Windows Live ID password" and a subheading "Use this form if someone you know asked you to help recover his or her Live ID account." Below this is a form with two sections. The first section is labeled "Your email address:" and contains the text "chris.marlowe@live.com". Below this is a note: "If you have multiple email addresses, ask your friend which of your addresses he or she provided when selecting you as an account trustee and enter that address." The second section is labeled "Your friend's email address:" and contains the text "william1564@live.com". Below this is a note: "This is the email address of the Windows Live ID account (e.g. Hotmail) for which your friend has forgotten the password." At the bottom of the form is a "Next" button. The footer of the page includes "© 2008 Microsoft | Privacy | Legal" and "Help Central | Feedback". The status bar at the bottom shows "Done", "Internet | Protected Mode: On", and "100%".

Windows Live ID Account Recovery - Windows Internet Explorer

http://recover.live.com/

Live Search

Windows Live ID Account Recovery

Help a friend reset his or her Windows Live ID password

Use this form if someone you know asked you to help recover his or her Live ID account.

Windows Live ID is the user identification system for Windows Live services such as Hotmail.

Your email address: chris.marlowe@live.com

If you have multiple email addresses, ask your friend which of your addresses he or she provided when selecting you as an account trustee and enter that address.

What is an account trustee?

Your friend's email address: william1564@live.com

This is the email address of the Windows Live ID account (e.g. Hotmail) for which your friend has forgotten the password.

Next

You will only be able to assist friends who have already identified you as one of their password-recovery trustees in their Windows Live ID profiles.

© 2008 Microsoft | Privacy | Legal

Help Central | Feedback

Done

Internet | Protected Mode: On

100%

Schecter et al. 2008

MS Live (proposed)—social backup authentication


Workable backup authentication

Please confirm your identity

Friend 2 of 7

- ☐ Kassie
- ☐ Sara
- ☐ Harrison
- ☐ Trista
- ☐ Lauren
- ☐ Laura
- ☐ I'm not sure

Go to Next Photo



Facebook—social questions backup

Workable backup authentication

Account Activity

View your recent account activity. If you notice an unfamiliar device or location, click "end activity"

Note: Locations and device types reflect our best guesses based on your ISP or wireless carrier.

Most Recent Activity

Last Accessed: **Today at 3:12pm**
Location: [Cambridge, ENG, GB \(Approximate\)](#)
Device Type: Firefox on Linux

Also Active

Last Accessed: **Yesterday at 6:54pm** [end activity](#)
Location: [Cambridge, ENG, GB \(Approximate\)](#)
Device Type: Mozilla/5.0 (X11; U; Linux i686; en-US; AppleWebKit/534.12 (KHTML, like Gecko) Ubuntu/9.10 Chromium/9.0.576.0 Chrome/9.0.576.0 Safari/534.12

Last Accessed: **November 1 at 2:12pm** [end activity](#)
Location: [London, ENG, GB \(Approximate\)](#)
Device Type: Chrome on Win7

Last Accessed: **October 29 at 8:17pm** [end activity](#)
Location: [Cambridge, ENG, GB \(Approximate\)](#)
Device Type: Mozilla/5.0 (X11; U; Linux i686; en-US; AppleWebKit/534.11 (KHTML, like Gecko) Ubuntu/9.10 Chromium/9.0.566.0 Chrome/9.0.566.0 Safari/534.11

Last Accessed: **October 24 at 1:26am** [end activity](#)
Location: [Cambridge, ENG, GB \(Approximate\)](#)
Device Type: Firefox on Linux

Facebook—social questions backup

jcb82@cl.cam.ac.uk