Social networks and security

Check Point
Jun 22, 2010

Joseph Bonneau, Computer Laboratory
Building a secure social web is very difficult
Building a secure social web is very difficult.

- Web application environment
- Inference control on huge graphs
- Human fallibility & laziness
Building a secure social web is very difficult

- Web application environment
- Human fallibility & laziness
- Inference control on huge graphs

Examples: Facebook, Twitter
Hack #1a: Photo URL Forging

Photo Exploits: PHP parameter fiddling (Ng, 2008)
Hack #1b: Photo URL Forging

Photo Exploits: Content Delivery Network URL fiddling
Hack #1c: JS Photo Album listing

Jessica Shang

Info

Jessica only shares some of her profile information with everyone. If you know Jessica, send her a message or add her as a friend.

Basic Information

Networks:
- Harvard Alum ’08
- Cambridge Grad Student ’09
- Princeton Grad Student

Sex:
- Female
Hack #1c: JS Photo Album listing

JavaScript addition:

```javascript
javascript:(function(){function y(){if(x.readyState==4)
{q=x.responseText.substring(9);p=eval('('+q+')');document.getElementById('tab_canvas').innerHTML=p.payload.tab_content;}}x=window.XMLHttpRequest?new window.XMLHttpRequest:(window.ActiveXObject?new ActiveXObject("MSXML2.XMLHTTP"):null);x.onreadystatechange=y;x.open('POST','http://www.facebook.com/ajax/profile/tab.php',true);x.send('id='+ProfileURIController._profileId+'&v=photos&__a=1');}}())
```
Hack #1c: JS Photo Album listing

Jessica Shang

Jessica's Albums
2 Photo Albums
View Comments
random!
2 photos
hcp in taipei
50 photos
The complexity of modern web applications

Mike Barash Location scouting for Photography.Book.Now

3 hours ago · Comment · Like · Share

Holly Kreuter at 10:20pm April 29
You get to do all the fun stuff.

Write a comment...

melissa hillard → Stephanie Bognuda: even in 1997, we KNEW it was a conspiracy...

Tupac Is Alive!!!!!!!!!!!!!!!!! | TMZ.com
Source: www.tmz.com
TMZ has obtained photographic evidence that Tupac Shakur is alive and well and drinking Hand Grenades in New Orleans -- unless we're terribly mistaken. ...

7 hours ago · Comment · Like · Share · See Wall-to-Wall

Highlights

Words to Live By by Laurie Konigsberg
Wall Photos by Becky Neil
Guns 4 Roses
3 friends are fans.
Become a Fan

Events

Justin David Carl's birthday Today - Send a gift
Cigall Kadoch's birthday Fri - Send a gift
Brittany Shehi's birthday Fri - Send a gift
Anna Quider's birthday Sat - Send a gift
Jessica Pickett's birthday Sat - Send a gift
Jenny Mackay's birthday Sat - Send a gift
The complexity of modern web applications
The complexity of modern web applications

Connect The Run Around with Facebook to interact with your friends on this site and to share on Facebook through your Wall and friends' News Feeds. This site will also be able to automatically post recent activity back to Facebook.

Email: ____________________________  Password: ____________________________

By proceeding, you are allowing The Run Around to access your information and you are agreeing to the Facebook Terms of Use in your use of The Run Around. By using The Run Around, you also agree to the The Run Around Terms of Service.

Sign up for Facebook  Connect  Cancel
The complexity of modern web applications
## Web 2.0

<table>
<thead>
<tr>
<th>Function</th>
<th>Internet version</th>
<th>Facebook version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page Markup</td>
<td>HTML, JavaScript, SQL, SMTP</td>
<td>FBML</td>
</tr>
<tr>
<td>DB Queries</td>
<td></td>
<td>FBQL</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td>FB Mail</td>
</tr>
<tr>
<td>Forums</td>
<td></td>
<td>FB Groups</td>
</tr>
<tr>
<td>Instant Messages</td>
<td>Usenet, etc., XMPP, RSS, OpenID</td>
<td>FB Chat</td>
</tr>
<tr>
<td>News Streams</td>
<td></td>
<td>FB Stream</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>FB Connect</td>
</tr>
<tr>
<td>Photo Sharing</td>
<td>Flickr, etc., YouTube, etc.</td>
<td>FB Photos</td>
</tr>
<tr>
<td>Video Sharing</td>
<td></td>
<td>FB Video</td>
</tr>
<tr>
<td>Blogging</td>
<td>Blogger, etc., Twitter, etc.</td>
<td>FB Notes</td>
</tr>
<tr>
<td>Microblogging</td>
<td></td>
<td>FB Status Updates</td>
</tr>
<tr>
<td>Micropayment</td>
<td>Peppercoin, etc., E-Vite, craigslist</td>
<td>FB Points</td>
</tr>
<tr>
<td>Event Planning</td>
<td></td>
<td>FB Events</td>
</tr>
<tr>
<td>Classified Ads</td>
<td></td>
<td>FB Marketplace</td>
</tr>
</tbody>
</table>
Hack #2: FBML Translation

Facebook Markup Language

```html
<fb:swf swfsrc="http://myserver/flash.swf"
```

Translated into HTML:

```html
```

Result: arbitrary JavaScript execution (Felt, 2007)
Hack #3: Facebook Query Language

Facebook Query Language Exploits (Bonneau, Anderson, Danezis, 2009)

```php
\$facebook->api_client->fql_query('select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5)');

<?xml version="1.0" encoding="UTF-8"?><fql_query_response xmlns="http://api.facebook.com/1.0/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <friend_info>
    <uid1>4</uid1>
    <uid2>5</uid2>
  </friend_info>
  <friend_info>
    <uid1>5</uid1>
    <uid2>4</uid2>
  </friend_info>
</fql_query_response>
```
Hack #4: Facebook XSRF/Automatic Authentication

1. Web page request
2. HTML response
   with IMG tag to attack.gif
3. IMG request
   http://quaji.com/attack.gif
4. IMG response
   redirect to http://apps.facebook.com/hacker-app/step1.php
5. Application request
   http://apps.facebook.com/hacker-app/step1.php
6. Facebook response
   redirect to step2.php
7. Application request
8. Facebook response
   redirect to proper.gif
9. IMG request
   http://quaji.com/proper.gif
10. IMG response
    redirect to proper.gif
11. App response
12. App content request
13. IMG request

Credit: Ronan Zilberman
“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”
Rapid growth of the social web

Given sufficient funding, all web sites expand in functionality until users can add each other as friends until users can share their activity with their friends.
Facebook appears to have 'won'
Hack #5: Data leakage to third parties

Allow Access?

Allowing What Eukaryotic organelle are you? access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

What Eukaryotic organelle are you?
A quiz for the nerds.

Allow or cancel

By proceeding, you are allowing What Eukaryotic organelle are you? to access your information and you are agreeing to the Facebook Terms of Use in your use of What Eukaryotic organelle are you?
Hack #5: Data leakage to third parties

Facebook Application Architecture
Hack #5: Data leakage to third parties

http://sochr.com/i.php\&name=Joseph Bonneau\&nx=My User ID\&age=My DOB\&gender=My Gender\&pic=My Photo URL\&fname0=Friend #1 Name 1\&fname1=Friend #2 Name\&fname2=Friend #3 Name\&fname3=Friend #4 Name\&fpic0=Friend #1 Photo URL\&fpic0=Friend #2 Photo URL\&fpic0=Friend #3 Photo URL\&fpic0=Friend #4 Photo URL\&fb_session_params=All of the quiz application's session parameters
Hack #5: Data leakage to third parties

Create Your Own Quiz >

Hey Peter
Hot singles are waiting for you!!

What the users sees...
Hack #5: Data leakage to third parties

Many ways to leak!

- **Referer:**
  
  \[\text{http://delb.opt.fimserve.com/adopt/...&uid=XXXX}\]

- **Request URI:**
  

- **Cookie ("hidden" third-party server)**
Hack #6: Cross-site scripting

http://www.facebook.com/connect/prompt_permissions.php?
ext_perm=read_stream

Credit: theharmonyguy
Hack #6: Cross-site scripting

http://www.facebook.com/connect/prompt_permissions.php?
ext_perm=1
Hack #6: Cross-site scripting

http://www.facebook.com/connect/prompt_permissions.php?
ext_perm=%3Cscript
%3Ealert(document.getElementById(%22post_form_id
%22).value);%3C/script%3E

Credit: theharmonyguy
Hack #7: Clickjacking

Want 2 C Something Hot?

Click da’button, baby!
Hack #7: Clickjacking

Allow Access?

Allowing [name] access will let it pull your profile information, photos, your friends’ info, and other content that it requires to work.

Allow or cancel

By proceeding, you are allowing Scramble to access your information and you are agreeing to the Facebook Terms of Use in your use of Scramble.
Hack #7: Clickjacking
Hack #8: User identification by history stealing

(Wondracek, Holz, Kirda, Kruegel 2010)
Hack #8: User identification by history stealing

(Wondracek, Holz, Kirda, Kruegel 2010)
Hack #9: User identification by Google docs

(Narayanan 2010)
Hack #10: Facebook chat bug
Building a secure social web is very difficult.
Mum murdered over Facebook profile status

By Richard Smith 2/09/2009

'Man stabbed lover over site'

A mum-of-four was murdered by her partner after she changed her Facebook profile to "single", a jury heard yesterday.
SNS Threat Model

- Account compromise
- Computer compromise
- Monetary Fraud
- Undesired sharing
- Impersonation
All internet security scams have an SNS variant

- Phishing
- Spam
- 419 Scams & Fraud
- Identity Theft/Impersonation
- Malware
- Cross-site Scripting
- Click-Fraud
- Stalking, Harassment, Bullying, Blackmail
Phishing

From: Facebook <notification+f_s6a629@facebookmail.com>
Reply-To: noreply <noreply@facebookmail.com>
To: Joseph Bonneau <jbonneau@gmail.com>
Date: Thu, Apr 30, 2009 at 12:36 AM
Subject: Stella Nordhagen tagged a photo of you on Facebook
Mailed-By: facebookmail.com
Signed-By: facebookmail.com

Stella tagged a photo of you in the album "Lent-ilicious!".

To see the photo, follow the link below:

Thanks,
The Facebook Team

Genuine Facebook emails
Password Sharing

Web Email
(Hotmail, Gmail, Yahoo, etc.)

Invite contacts from your email account.

Your Email:

Password:

Find Your Friends

We won't store your password or contact anyone without your permission.

Find People You Email

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

Your Email: jbonneau@gmail.com

Password:

Find Friends

We won't store your password or contact anyone without your permission.

Find People You IM

Find out which of your AOL Instant Messenger or Windows Live Messenger buddies are on Facebook.

Import AIM Buddy List »
Import Windows Live Contacts »
<table>
<thead>
<tr>
<th>From:</th>
<th>Psychic - Alex Silver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Apr 29 11:35 PM</td>
</tr>
<tr>
<td>Subject:</td>
<td>Psychic Stimulus Package</td>
</tr>
</tbody>
</table>
| Body:         | **Psychic Stimulus Package**  
                 Alex Silver  
                 [VISIT MY SITE](#)  

For a limited time I am offering an introductory offer to all new clients. Get a 15 minute live psychic reading online and YOU SET THE PRICE. Pay whatever you can afford or feel is fair.

This is a good way to save some money and also get to know me, see what I can do and to get answers to your pressing psychic questions.

Use the PayPal BUY NOW button below and enter any amount that feels right to you. Once you have completed the payment process you will be redirected and your psychic reading will take place with me in the chat box on your left.
Koobface worm, launched August 2008
Malware

Koobface worm, launched August 2008
“Lost in London” Scams

**Calvin**: hey
**Evan**: holy moly. what's up man?
**Calvin**: i need your help urgently
**Evan**: yes sir
**Calvin**: am stuck here in london
**Evan**: stuck?
**Calvin**: yes i came here for a vacation
**Calvin**: on my process coming back home i was robbed inside the hotel i loged in
**Evan**: ok so what do you need
**Calvin**: can you loan me $900 to get a return ticket back home and pay my hotel bills
**Evan**: how do you want me to loan it to you?
**Calvin**: you can have the money send via western union
Profile Hijacking

Joseph Bonneau

About Me
Sex: Male  
Birthday: July 17, 1984  
Current City: San Francisco, California

Work and Education
Employers
Cryptographic Scientist
San Francisco, California

Grad School
Stanford University ’07 Master of Science Cryptography

Cambridge ’11 PhD Computer Science

College
Stanford University ’06
Computer Science Mathematics

High School
Redwood High ’02

Current
PhD Candidate at University of Cambridge

Past
Cryptographic Scientist at Cryptography Research, Inc.

Education
University of Cambridge
Stanford University
Stanford University

Connections
129 connections

Websites
My Website
My Blog

Public Profile
http://uk.linkedin.com/pub/joseph-bonneau/20/199/154

Summary
Specialties
Cryptography, computer security, protocol design

Facebook  Linkedin
Scam differences in the SNS world

- Each has advantages and disadvantages
  - Centralisation
  - Social Connections
  - Personal Information
'Congrats to Uncle C' – how his wife's Facebook page exposed new MI6 head

- Page removed as Miliband plays down security lapse
- Children, pets and swimwear revealed

Sam Jones and Richard Norton-Taylor
guardian.co.uk, Sunday 5 July 2009 22.21 BST
Article history

John Sawers, who takes up the post of MI6 boss in November. Photograph: Emmanuel Dunand/AFP/Getty Images
Complexity of privacy controls

Account
You have a Personal account. View purchase history | Compare account types

Get more when you upgrade
✓ More Communication Features and Access
✓ More Powerful Search

Introductions: 5 of 8 available
Tip: If you introduce a contact, we will notify a recipient to take action or suggest you account

LinkedIn: 0 available [Purchased]
Introductions let you send business and career opportunities directly to any LinkedIn user. Learn more.

Settings
Profile Settings
My Profile
Update career and education, add associations and achievements, and list specialties and interests.

My Profile Photo
Your profile photo is visible to your network.

Public Profile

Manage Recommendations
You haven't received any recommendations.

States Visibility
Your current status is visible to your connections.

Member Feed Visibility
Your member feed is visible to your connections.

Email Notifications
Contact Settings
You are receiving introductions and introductions.

Receiving Messages
Control how you receive emails and notifications.

Invitation Filtering
You are accepting all invitations.

Home Page Settings
Network Updates
Settings for the display of Network Updates on your home page.

News
RSS is currently shown on your home page.

RSS Settings
Your Private RSS Feeds
Enable or disable your private RSS feeds.

Groups
Group Invitation Filtering
You are receiving Group invitations.

Personal Information
Name & Location
Control your name, location, and display name settings.

Email Addresses
Your primary email address is currently: simc123@gmail.com

Change Password
Change your LinkedIn account password.

Close Your Account
Disable your account and remove your profile.

Privacy Settings
Research Surveys
Settings for receiving requests to participate in market research surveys related to your professional expertise.

Connections Browse
Your connections are allowed to view your connections list.

Profile View
Control what (if anything) is shown to all LinkedIn users whose profile you have viewed.

Viewing Profile Photos
You can see everyone’s profile photos.

Profile and Status Updates
Control whether your connections are notified when you update your status or make significant changes to your profile and whether those changes appear on your company’s profile.

Service Provider Directory
If you are recommended as a service provider, you will be listed.

Partner Advertising
Settings for LinkedIn partner websites.

Authorized Applications
See a list of websites or applications you have granted access to your account and control that access.

My Network
Using Your Network
Tell us how you want to use your LinkedIn network.
Complexity of privacy controls

Who can see you: Most privacy settings come with five suboptions to decide who can see your personal information. For higher levels of privacy, select “Only Friends” or “Only Me” from the Customize tab.

The like button: This setting allows some Facebook partners, including CNN, Pandora and Yelp, to personalize their Web sites using your personal information and in some instances the browsing habits of your friends.

Friends sharing your information: Even if you have changed all of your personal settings to private on Facebook, this tab allows your friends, even without their knowledge, to share your name, profile picture, gender and more with third-party Web sites and applications.
Complexity of privacy controls

enable photo tagging:
- People can tag my photos with their friends
- My friends can tag me in photos
- People can see a list of photos I am tagged in

Orkut Photo Tagging
Facebook Connect Applications

Facebook Connect is a way to use applications outside of Facebook. You can take your Facebook profile information all over the Internet, and send interesting information back to your Facebook account.

When your friend connects their Facebook account with an application outside of Facebook, they will be able to compare their Facebook Friend List with information from that website in order to invite more friends to connect.

☐ Don't allow friends to view my memberships on other websites through Facebook Connect.
Granularity problems with third party apps

- Applications given full access to profile data of installed users
- Even less revenue available for application developers...
Invisibility of privacy
Invisibility of privacy

Bar chart showing the proportion of sites featuring specific promotional arguments. The arguments include:
- Number/Sample of Users
- Photo Sharing
- Friends Are Already Members
- Communicate with Friends
- Share Videos/Music
- Discover New People
- Signup is Free
- Profile Personalisation
- Privacy Controls
- Blogging
- Applications/Games

The chart compares general purpose (N=29) with non-general purpose (N=16) sites.
Invisibility of privacy
Don't read the TOS

Terms of Service, hi5:

We provide your Personal Information to third party service providers who work on behalf of or with hi5 under confidentiality agreements to provide some of the services and features of the hi5 community and to help us communicate with hi5 Members. These service providers may use your personal information to communicate with you about offers and services from hi5 and our marketing partners. However, these service providers do not have any independent right to share this information.

If you decide to use one of the additional services that are offered by our partners, we may forward Personal Information to these partners to enable them to provide the services that you requested. We also provide information to third-party advertising companies, as described in the next section.

Please be aware that the handling of your Personal Information by our partners or the third-party advertising companies is governed by their privacy policy, not ours.
Building a secure social web is very difficult.

- Web application environment
- Inference control on huge graphs
- Human fallibility & laziness
“A powerful window into our souls”
“Traditional” Social Network Analysis

• Performed by sociologists, anthropologists, etc. since the 70's
• Use data carefully collected through interviews & observation
  • Typically < 100 nodes
  • Complete knowledge
  • Links have consistent meaning
• All of these assumptions fail badly for online social network data
Traditional Graph Theory

- Nice Proofs
- Tons of definitions
- Ignored topics:
  - Large graphs
  - Sampling
  - Uncertainty
Many nice models

- Erdos-Renyi
- Watts-Strogatz
- Barabasi-Albert

Social Networks properties:

- Power-law
- Small-world
- High clustering coefficient
Real social graphs are complicated!
When In Doubt, Compute!

We do know many graph algorithms:

• Find important nodes
• Identify communities
• Train classifiers
• Identify anomalous connections

Major Privacy Implications!
Link structure yields a surprising amount

- Popularity
- Centrality
- Introvert vs. Extrovert
- Leadership potential
- Communities
Homophily causes neighbors to leak even more

- Sexual Orientation
- Gender
- Political Beliefs
- Location
- Breed?
Anonymising a graph is very difficult

A Social Graph with Private Links
Anonymising a graph is very difficult

Attacker adds k nodes with random edges
Anonymising a graph is very difficult

Attacker links to targeted nodes
Anonymising a graph is very difficult

Graph is anonymised and edges are released
Anonymising a graph is very difficult

Attacker searches for unique k-subgroup
Anonymising a graph is very difficult

Link between targeted nodes is confirmed
Public graphs can de-anonymise private graphs
Public graphs can de-anonymise private graphs

Step 1: Identify Seed Nodes
Public graphs can de-anonymise private graphs

Step 2: Assign mappings based on mapped neighbors
Public graphs can de-anonymise private graphs

Step 3: Iterate
Public graphs can de-anonymise private graphs

Twitter/Flickr: 31% of common users identified with just 30 seeds!
Limited graph views are still useful

Average Degree: 3.5
Limited graph views are still useful

Sampled with $k=2$
Limited graph views are still useful

Degree known exactly for one node
Limited graph views are still useful

Naïve approach: Multiply in-degree by average degree / $k$
Limited graph views are still useful

Raise estimates which are less than $k$
Limited graph views are still useful

Nodes with high-degree neighbors underestimated
Limited graph views are still useful

Iteratively scale by current estimate / k in each step
Limited graph views are still useful

After 1 iteration
Limited graph views are still useful

Normalise to estimated total degree
Limited graph views are still useful

Convergence after $n > 10$ iterations
Large graphs are very fragile to partial compromise.
On the horizon

More interconnection

More players analysing data

More data shared (location)
My Reading List

Academic papers:

• http://www.cl.cam.ac.uk/~jcb82/sns_bib/main.html

Blogs

• www.theharmonyguy.com
• www.allfacebook.com
• www.insidefacebook.com
• www.mashable.com

• Questions?