Unique Security Challenges for Online Social Networks

ICT-Forward 2009
May 4, 2009

Joseph Bonneau, Computer Laboratory
Pessimistic View of Social Networks

Just LAMP websites where you list your friends...
The Surprising Depth of Facebook

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.

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

Facebook Stream
The Surprising Depth of Facebook

Facebook Applications

Round ends in: 0:39

My Score: 153  My Best: 310

LEARS is worth 4

Enter

Words Remaining

<table>
<thead>
<tr>
<th>3LW</th>
<th>4LW</th>
<th>5LW</th>
<th>6LW</th>
<th>7LW</th>
<th>8LW</th>
</tr>
</thead>
<tbody>
<tr>
<td>74</td>
<td>105</td>
<td>96</td>
<td>49</td>
<td>27</td>
<td>9</td>
</tr>
</tbody>
</table>

Possible Score: 1466 pts

Words you've found:

- LEARS (4)
- LEAR (2)
- TARTS (4)
- TART (2)
- LEANER (6)
- LEAN (2)
- LNMT (2)

End this Round

My Friends

- Nan Gao 1st 416 pts
- Adrienne Clark 6th 199 pts
- Julie Zhuo 7th 199 pts
- Jessica Shang 9th 147 pts

CURRENT SCORE

8th 153 pts
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, 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>
Facebook has essentially re-invented the Internet
- Simpler (mostly)
- Centralised
- Proprietary
- Walled

Killer addition is social context
“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”
Why I Care About Social Networks

• Defining Characteristic of Generation Y (Born after 1980)
  - This generation's “Public Space” (boyd, 2007)
• American teens average 30 minutes per day
  - Also this generation's TV
• I was a Facebook early adopter in 2004
Why I Care About Social Networks

Still fairly dominated by youth
Why Everyone Will Care About Social Networks

Rapid growth

Facebook - Total Active Users

InsideFacebook.com
Why Everyone Will Care About Social Networks

Rapid growth in older demographics
Why Everyone Will Care About Social Networks

Rapid international growth

<table>
<thead>
<tr>
<th>Country</th>
<th>10/8/08</th>
<th>3Q08 Growth</th>
<th>2008 Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>32,975,440</td>
<td>16%</td>
<td>94%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>12,410,520</td>
<td>9%</td>
<td>43%</td>
</tr>
<tr>
<td>Canada</td>
<td>9,324,600</td>
<td>-2%</td>
<td>7%</td>
</tr>
<tr>
<td>Turkey</td>
<td>4,921,980</td>
<td>41%</td>
<td>73%</td>
</tr>
<tr>
<td>Chile</td>
<td>3,682,680</td>
<td>50%</td>
<td>3343%</td>
</tr>
<tr>
<td>France</td>
<td>3,622,960</td>
<td>48%</td>
<td>183%</td>
</tr>
<tr>
<td>Australia</td>
<td>3,559,380</td>
<td>6%</td>
<td>52%</td>
</tr>
<tr>
<td>Colombia</td>
<td>3,304,600</td>
<td>23%</td>
<td>325%</td>
</tr>
<tr>
<td>Venezuela</td>
<td>1,591,220</td>
<td>48%</td>
<td>1061%</td>
</tr>
<tr>
<td>Italy</td>
<td>1,342,600</td>
<td>135%</td>
<td>460%</td>
</tr>
<tr>
<td>Sweden</td>
<td>1,324,060</td>
<td>16%</td>
<td>21%</td>
</tr>
<tr>
<td>Denmark</td>
<td>1,244,700</td>
<td>58%</td>
<td>204%</td>
</tr>
<tr>
<td>Norway</td>
<td>1,227,260</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Spain</td>
<td>1,214,200</td>
<td>57%</td>
<td>265%</td>
</tr>
<tr>
<td>Mexico</td>
<td>1,168,320</td>
<td>6%</td>
<td>80%</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>1,134,860</td>
<td>24%</td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>1,094,780</td>
<td>114%</td>
<td>1033%</td>
</tr>
<tr>
<td>South Africa</td>
<td>961,720</td>
<td>-1%</td>
<td>31%</td>
</tr>
<tr>
<td>Belgium</td>
<td>925,600</td>
<td>78%</td>
<td>258%</td>
</tr>
<tr>
<td>Germany</td>
<td>860,460</td>
<td>24%</td>
<td>79%</td>
</tr>
<tr>
<td>India</td>
<td>794,440</td>
<td>3%</td>
<td>47%</td>
</tr>
<tr>
<td>Egypt</td>
<td>791,440</td>
<td>-1%</td>
<td>29%</td>
</tr>
<tr>
<td>Switzerland</td>
<td>701,420</td>
<td>67%</td>
<td>217%</td>
</tr>
<tr>
<td>Finland</td>
<td>680,780</td>
<td>26%</td>
<td>58%</td>
</tr>
<tr>
<td>Greece</td>
<td>663,920</td>
<td>28%</td>
<td>260%</td>
</tr>
</tbody>
</table>

Rapid international growth
Facebook is Everywhere...

Freetown Christiania (Copenhagen, Denmark)
Facebook is Far From the Only SNS

Most popular services around the world:
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
### 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</td>
<td>FBML</td>
</tr>
<tr>
<td>DB Queries</td>
<td>SQL</td>
<td>FBQL</td>
</tr>
<tr>
<td>Email</td>
<td>SMTP</td>
<td>FB Mail</td>
</tr>
<tr>
<td>Forums</td>
<td>Usenet, etc.</td>
<td>FB Groups</td>
</tr>
<tr>
<td>Instant Messages</td>
<td>XMPP</td>
<td>FB Chat</td>
</tr>
<tr>
<td>News Streams</td>
<td>RSS</td>
<td>FB Stream</td>
</tr>
<tr>
<td>Authentication</td>
<td>OpenID</td>
<td>FB Connect</td>
</tr>
<tr>
<td>Photo Sharing</td>
<td>Flickr, etc.</td>
<td>FB Photos</td>
</tr>
<tr>
<td>Video Sharing</td>
<td>YouTube, etc.</td>
<td>FB Video</td>
</tr>
<tr>
<td>Blogging</td>
<td>Blogger, etc.</td>
<td>FB Notes</td>
</tr>
<tr>
<td>Microblogging</td>
<td>Twitter, etc.</td>
<td>FB Status Updates</td>
</tr>
<tr>
<td>Micropayment</td>
<td>Peppercoin, etc.</td>
<td>FB Points</td>
</tr>
<tr>
<td>Event Planning</td>
<td>E-Vite</td>
<td>FB Events</td>
</tr>
<tr>
<td>Classified Ads</td>
<td>craigslist</td>
<td>FB Marketplace</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

- The Elephant in the Room
  - Privacy
Differences in the SNS world

- Each has advantages and disadvantages
  - Centralisation
  - Social Connections
  - Personal Information
  - Economic Uncertainty
Security
Major Security Threats

- Account compromise
  - Email or SNS (practically the same)
- Computer compromise
- Monetary Fraud
- Service denial
  - Making the site useless
Phishing

Genuine Facebook emails

Star 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-licious!".

To see the photo, follow the link below:

Thanks,
The Facebook Team
Phishing attempt, April 30, 2009

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=113998996147&mid=63b67eG334d4G1da651eG0
Phishing attempt, April 30, 2009
Phishing

- Major Phishing attempts, April 29-30, 2009
  - Simple “look at this” messages
  - Phished credentials used to automatically log in, send more mail
  - Some users report passwords changed
- Most “elaborate” scheme seen yet
- Phishtank reports Facebook 7th most common target
  - Behind only banks, PayPal, eBay
Why SNSs are Vulnerable to Phishing

- “Social Phishing” is far more effective
  - 72% successful in controlled study (Jagatic et al.)
- No TLS for login page
- No anti-phishing measures
- Frequent genuine emails with login-links
- Users don't consider SNS password as valuable
- Web 2.0 sites encourage password sharing...
Password Sharing

Invite Your Friends

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: 

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 »
SNS Phishing Defense

• Many advantages over email phishing prevention
  - Real-time monitoring
  - Can block, revoke messages
  - Block outgoing links
• Fast response to recent attacks
  - Emails blocked, removed, sites down within 24 hours
Malware

Koobface worm, launched August 2008
Malware

Koobface worm, launched August 2008
Malware

- Koobface worm, launched August 2008
  - Harvest Facebook accounts
  - Spreads through Facebook messages
- Similar to Phishing
  - Rapid spread via social context
  - SNS can use social context to detect
  - Also, warn users leaving site
Malware Defense

Be careful

For the safety and privacy of your Facebook account, remember to never enter your password unless you're on the real Facebook web site. Also be sure to only download software from sites you trust.

http://geocities.com/rubingallegos09?dchbb850=13191be140046e6d498e1ac0d07d218c

Continue  Cancel
Malware Defense

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.


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

[Go Back to MySpace](#)

[Don't show me this alert again.](#)
Attention all Facebook members.

Facebook is recently becoming very overpopulated. There have been many members complaining that Facebook is becoming very slow. Record shows that the reason is that there are too many non-active Facebook members. And on the other side too many new Facebook members. We will be sending this messages around to see if the Members are active or not. If you're active please send to 15 other users using Copy+Paste to show that you are active. Those who do not send this message within 2 weeks, the user will be deleted without hesitation to create more space. If Facebook is still overpopulated we kindly ask for donations but until then send this message to all your friends and make sure you send this message to show me that you are active and not deleted.

Founder of Facebook
Mark Zuckerberg
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
Scams

• Effective due to social context
  - Skilled impersonators should be able to do much better
• Not much can be done to prevent
  - Education
• Again, build detection system using social context, history
  - Unexpected log-ins
  - References to Western Union, etc.
Spam

• Major factor in the decline of MySpace, Friendster
• Attractive target
  - Can message any user in the system
  - “Social Spam” much more effective than random spam
  - Account creation is very cheap
<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>
<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.
Spam

- Many advantages for SNS
  - Global monitoring, blocking
  - Automatically detect spammer profiles
    - Analyse link history
    - Analyse graph structure
    - Analyse profile
- Aggressively request CAPTCHAs
- Legal: Facebook won US $873 M award
Spam

- Tough question: Spam vs. Viral Promotion?
- Facebook moving to two-classes of user:
  - User profiles bound to represent “real people”
    - Limits on friend count
    - Limits on usernames
    - Limits on messages
  - “Pages” for celebrities, companies, bands, charities, etc.
    - Most limits removed
    - Subject to stricter control
Common Trends

• Social channels increase susceptibility
  - Personal information also aids greatly in targeted attacks

• Fundamental issue: SNS environment leads to carelessness
  - Rapid, erratic browsing
  - 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
Privacy
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
Interested Parties

- Data Aggregation
  - Marketers, Insurers, Credit Ratings Agencies, Intelligence, etc.
  - SNS operator implicitly included
  - Often, graph information is more important than profiles
- Targeted Data Leaks
  - Employers, Universities, Fraudsters, Local Police, Friends, etc.
  - Usually care about profile data and photos
Major Privacy Problems

• Complicated privacy model
  - Settings confusing and open by default
• Implementation errors
  - Frequently unable to enforce model
• Economic pressure
  - SNS needs data sharing to grow and profit
Complicated Privacy Model

- Facebook has over 60 settings on 7 pages
  - 90% of users don't edit
- Open by default
- Many settings have unexpected interactions
Privacy Settings Confusion

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
Privacy Settings Confusion

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.
Implementation errors

- Extreme complexity
  - Especially with third-party applications and sites
  - Many moving parts written by different teams
- Extreme size
  - Content must be stored in third-party CDNs
- Sites built rapidly with privacy as an after-thought
- Long history of privacy-related bugs
Implementation errors

Facebook Markup Language

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

Translated into HTML:

```
<img src="http://facebook/cached-image.jpg" style="-moz-
binding:url('http://myserver/xssmoz.xml#xss');" />
```

Result: arbitrary JavaScript execution (Felt, 2007)
Implementation errors

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

Photo Exploits: PHP parameter fiddling (Ng, 2008)
Implementation errors

Photo Exploits: Content Delivery Network URL fiddling (Bonneau, 2009)
Economic Pressure

- Most SNSs still lose money
  - Advertising business model yet to prove its viability
- Grow first, monetize later
  - “Growth is primary, revenue is secondary” - Mark Zuckerberg
- Privacy is often an impediment to new features
  - Facebook Beacon
  - News feed
  - Site re-designs
- Applications given full access to profile data of installed users
- Even less revenue available for application developers...
Public Listings

Joseph Bonneau
Add as Friend | Send a Message | View Friends

Here are some of Joseph Bonneau's friends:

David Cottingham
Emma Alden
Aisling Byrne
Stella Nordhagen
David J Hornsby
Jillian Sullivan
Pedro Alejandro Ortega
Erik George Tsarpalis

Not the right Joseph Bonneau you were looking for? Search more
Public Listings provide enough graph data to approximate most functions (Bonneau, Anderson, Stajano, Anderson, 2009)
Terms of Service

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.

Most Terms of Service reserve broad rights to user data
Market Dynamics

- Sites avoid competing on privacy as a selling point
- Significant lock-in
- Enormous Network effects
- Privacy rarely mentioned during sign-up
  - Privacy salience reduces enjoyment of site
- Users can't determine which sites are better
  - Lemons market
Conclusions

• Social Networking coming to dominate the web
• Makes malicious behaviour more enticing
• Also aids prevention
• Privacy is still a mess
Questions?
Publications


- And several hacks on [www.lightbluetouchpaper.org](http://www.lightbluetouchpaper.org)