CS 290
Host-based Security and Malware

Christopher Kruegel

chris@cs.ucsb.edu

Social Networks

- Social networks
  - massive growth and rise in popularity
  - people provide significant amount of private/sensitive information
  - security and privacy threats not well understood
  - often, protection offered by social network providers lacking

Social Network Security Issues

- Data privacy
  - blackmail
  - identity theft
  - personalized spear-phishing
  - targeted advertisement

- New venue to reach large number of potential victims
  - spam
  - malware / worms
  - links that point to sites with browser exploits (drive-by downloads)

Social Network Security Issues

- Rogue applications
  - developed and under control of third parties
  - access to profile information and those of friends

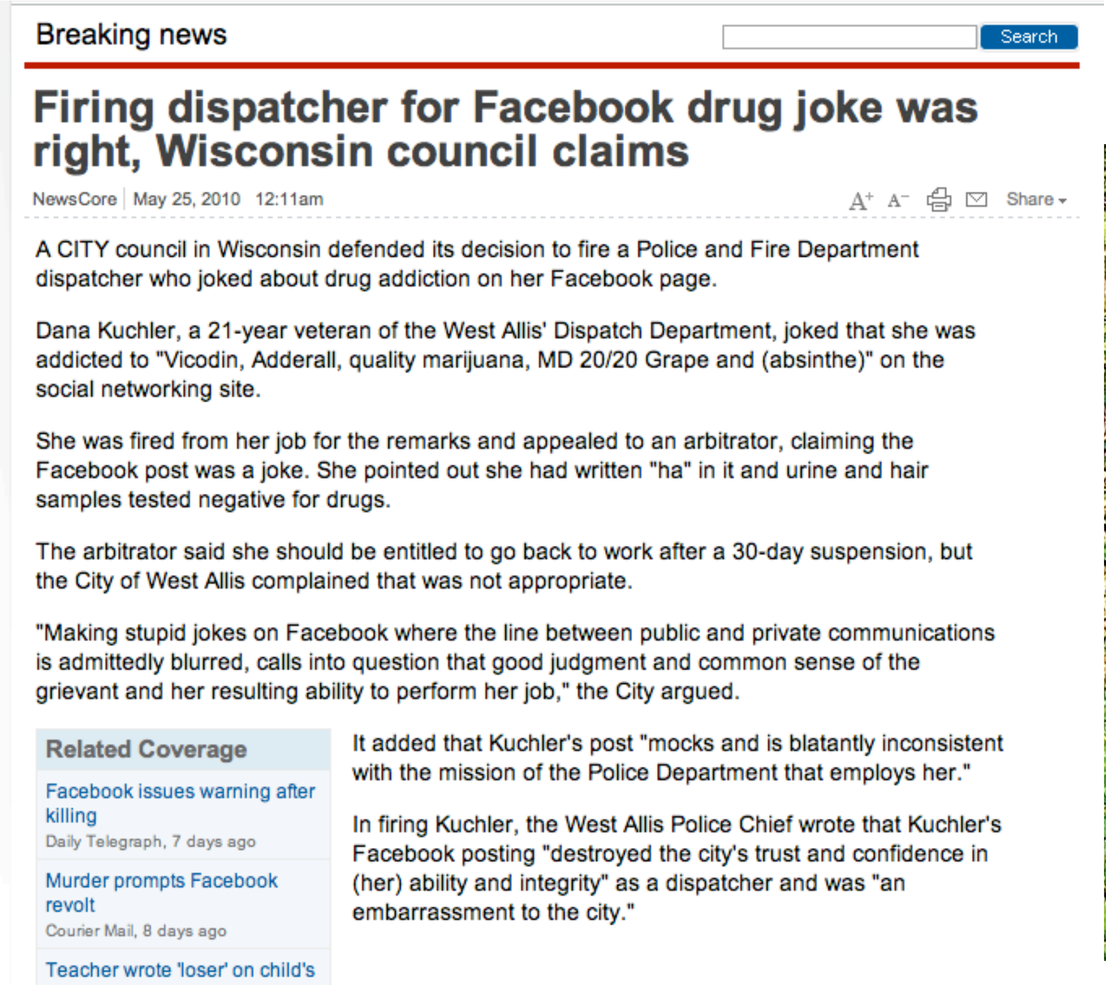
- Support for regular crime
  - absence notes for burglary opportunities
  - monitor victim’s spending habits

- Crawlers
  - obtain large amount of data against will of social networks

Social Network Security Issues

- Data privacy
  - blackmail
  - identity theft
  - personalized spear-phishing
  - targeted advertisement
- New venue to reach large number of potential victims
  - spam
  - malware / worms
  - links that point to sites with browser exploits (drive-by downloads)

Data Privacy



Breaking news

Firing dispatcher for Facebook drug joke was right, Wisconsin council claims

NewsCore | May 25, 2010 12:11am

A CITY council in Wisconsin defended its decision to fire a Police and Fire Department dispatcher who joked about drug addiction on her Facebook page.

Dana Kuchler, a 21-year veteran of the West Allis' Dispatch Department, joked that she was addicted to "Vicodin, Adderall, quality marijuana, MD 20/20 Grape and (absinthe)" on the social networking site.

She was fired from her job for the remarks and appealed to an arbitrator, claiming the Facebook post was a joke. She pointed out she had written "ha" in it and urine and hair samples tested negative for drugs.

The arbitrator said she should be entitled to go back to work after a 30-day suspension, but the City of West Allis complained that was not appropriate.

"Making stupid jokes on Facebook where the line between public and private communications is admittedly blurred, calls into question that good judgment and common sense of the grievant and her resulting ability to perform her job," the City argued.

It added that Kuchler's post "mocks and is blatantly inconsistent with the mission of the Police Department that employs her."

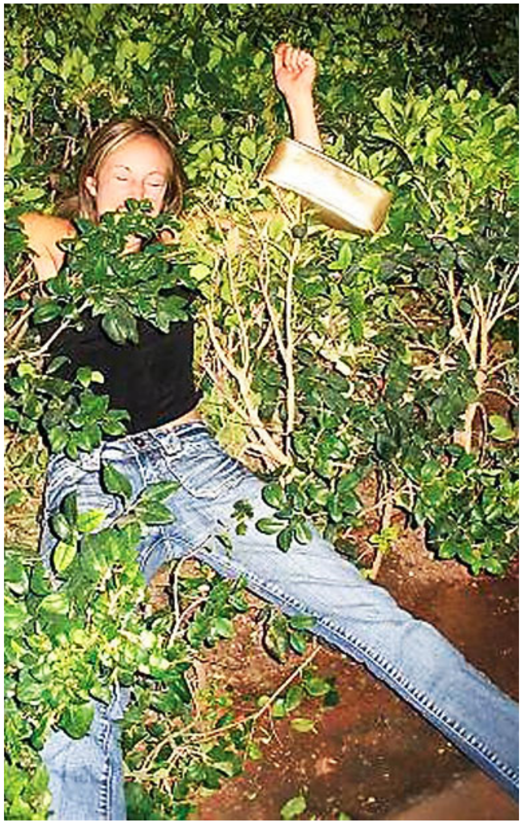
In firing Kuchler, the West Allis Police Chief wrote that Kuchler's Facebook posting "destroyed the city's trust and confidence in (her) ability and integrity" as a dispatcher and was "an embarrassment to the city."

Related Coverage

Facebook issues warning after killing
Daily Telegraph, 7 days ago

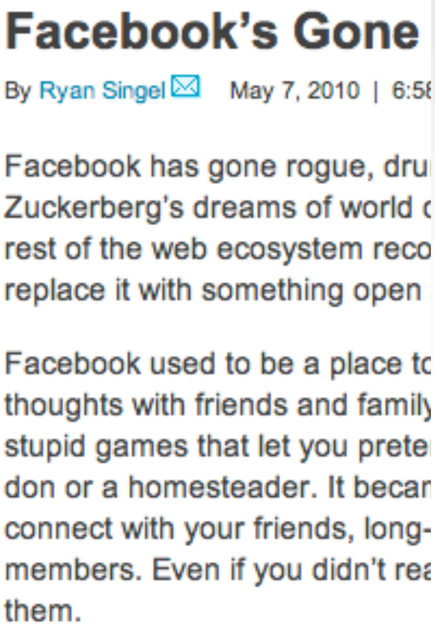
Murder prompts Facebook revolt
Courier Mail, 8 days ago

Teacher wrote 'loser' on child's



Data Privacy

- Wealth of sensitive and private information
  - not everything on Facebook is cool
  - so, how do social networks protect this data

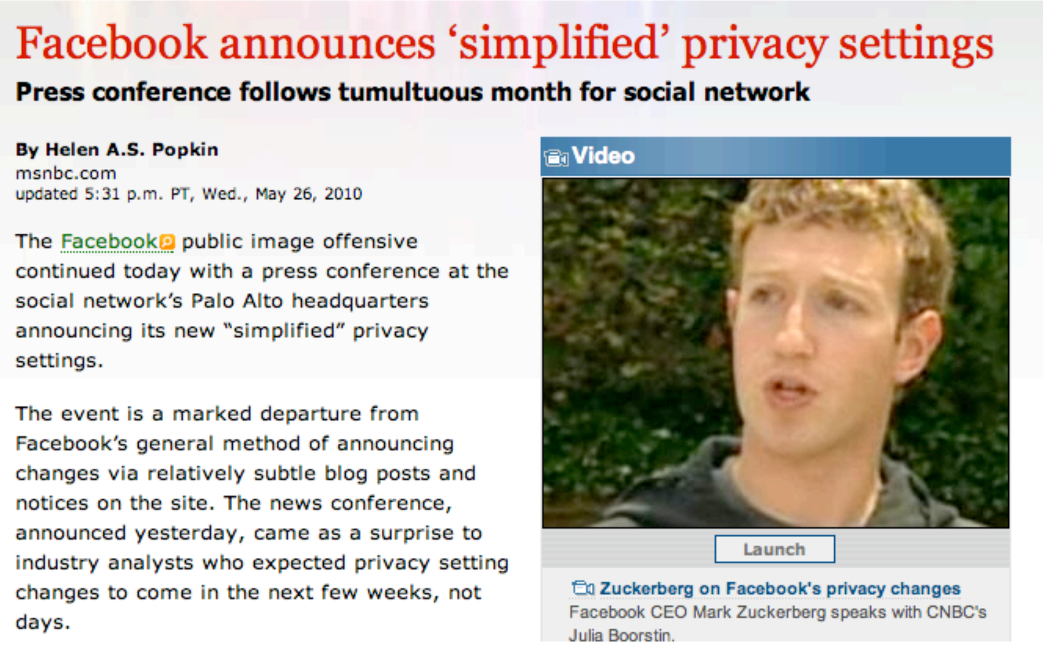


Facebook's Gone

By Ryan Singel May 7, 2010 | 6:5

Facebook has gone rogue, dru
Zuckerberg's dreams of world c
rest of the web ecosystem reco
replace it with something open

Facebook used to be a place to
thoughts with friends and family
stupid games that let you prete
don or a homesteader. It becar
connect with your friends, long-
members. Even if you didn't rea
them.



Facebook announces 'simplified' privacy settings

Press conference follows tumultuous month for social network

By Helen A.S. Popkin
msnbc.com
updated 5:31 p.m. PT, Wed., May 26, 2010

The Facebook public image offensive continued today with a press conference at the social network's Palo Alto headquarters announcing its new "simplified" privacy settings.

The event is a marked departure from Facebook's general method of announcing changes via relatively subtle blog posts and notices on the site. The news conference, announced yesterday, came as a surprise to industry analysts who expected privacy setting changes to come in the next few weeks, not days.

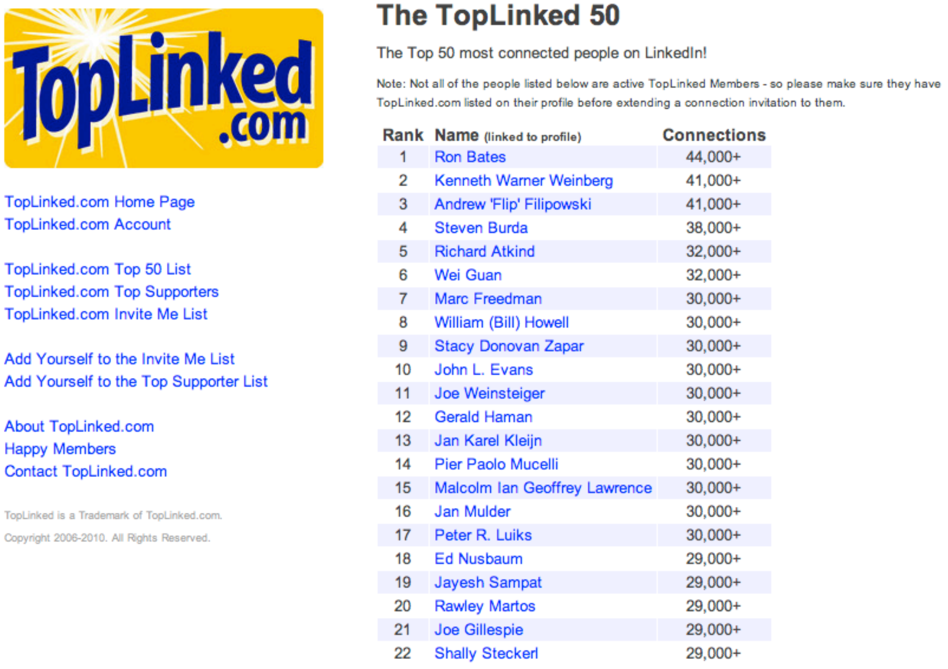
Zuckerberg on Facebook's privacy changes
Facebook CEO Mark Zuckerberg speaks with CNBC's Julia Boorstin.

Data Privacy

- Wealth of sensitive and private information
  - not everything on Facebook is cool
  - so, how do social networks protect this data

- Wait! You need to

- True, but …
  - open profiles
  - fake profiles
  - profile cloning
  - link addicts



TopLinked.com Home Page
TopLinked.com Account

TopLinked.com Top 50 List
TopLinked.com Top Supporters
TopLinked.com Invite Me List

Add Yourself to the Invite Me List
Add Yourself to the Top Supporter List

About TopLinked.com
Happy Members
Contact TopLinked.com

TopLinked is a Trademark of TopLinked.com.
Copyright 2006-2010. All Rights Reserved.

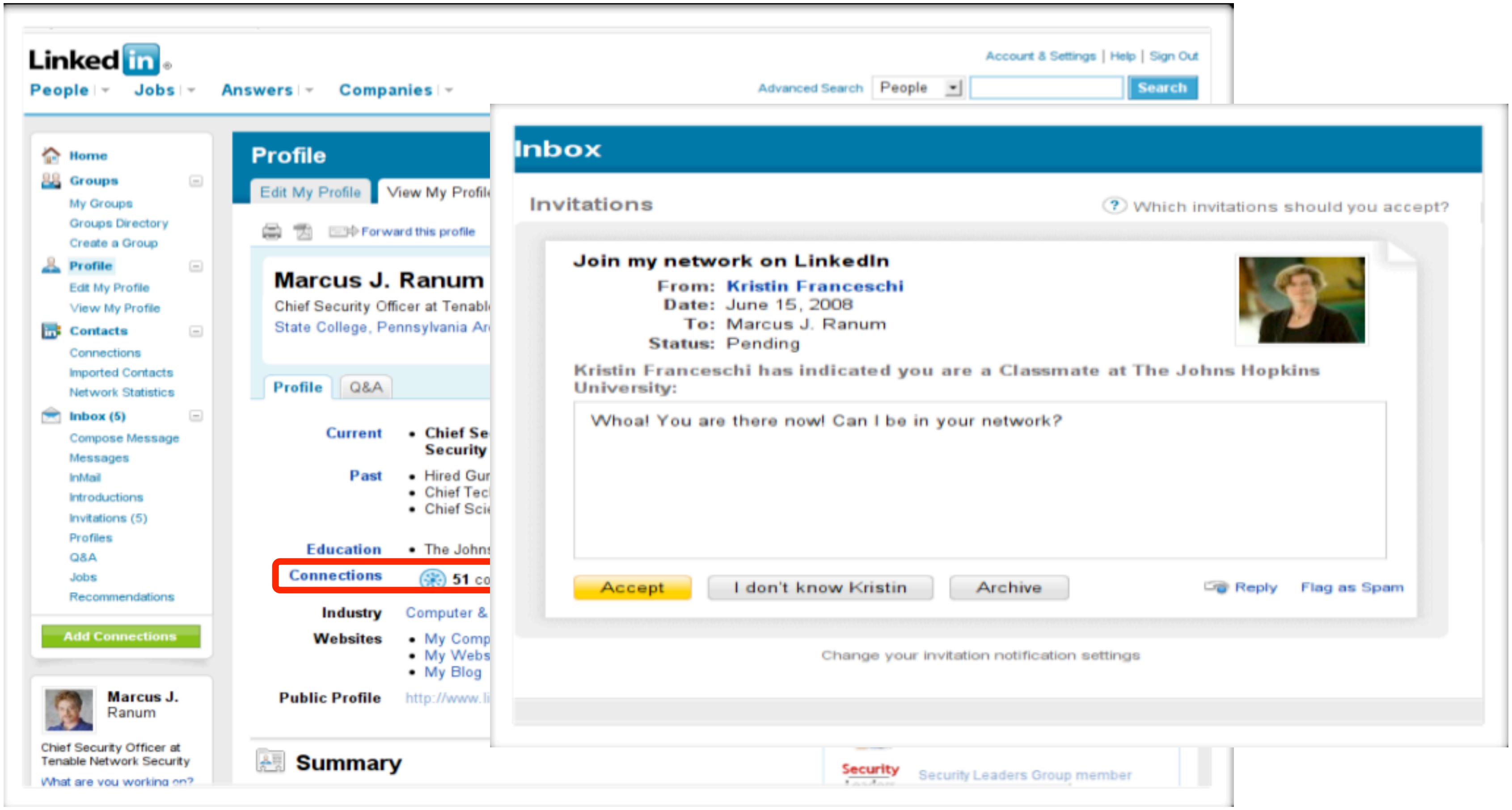
The TopLinked 50

The Top 50 most connected people on LinkedIn!

Note: Not all of the people listed below are active TopLinked Members - so please make sure they have TopLinked.com listed on their profile before extending a connection invitation to them.

Rank	Name (linked to profile)	Connections
1	Ron Bates	44,000+
2	Kenneth Warner Weinberg	41,000+
3	Andrew 'Flip' Filipowski	41,000+
4	Steven Burda	38,000+
5	Richard Atkind	32,000+
6	Wei Guan	32,000+
7	Marc Freedman	30,000+
8	William (Bill) Howell	30,000+
9	Stacy Donovan Zapar	30,000+
10	John L. Evans	30,000+
11	Joe Weinsteiger	30,000+
12	Gerald Haman	30,000+
13	Jan Karel Kleijn	30,000+
14	Pier Paolo Mucelli	30,000+
15	Malcolm Ian Geoffrey Lawrence	30,000+
16	Jan Mulder	30,000+
17	Peter R. Luiks	30,000+
18	Ed Nusbaum	29,000+
19	Jayesh Sampat	29,000+
20	Rawley Martos	29,000+
21	Joe Gillespie	29,000+
22	Shally Steckerl	29,000+

Fake Profile (Ranum Experiment)



Marcus J. Ranum

Chief Security Officer at Tenabl

State College, Pennsylvania Ar

Current • Chief Se Security

Past • Hired Gur • Chief Tec • Chief Sci

Education • The Johns

Connections 51 co

Industry Computer &

Websites • My Comp • My Webs • My Blog

Public Profile http://www.li

Marcus J. Ranum

Chief Security Officer at Tenable Network Security

What are you working on?

Join my network on LinkedIn

From: Kristin Franceschi

Date: June 15, 2008

To: Marcus J. Ranum

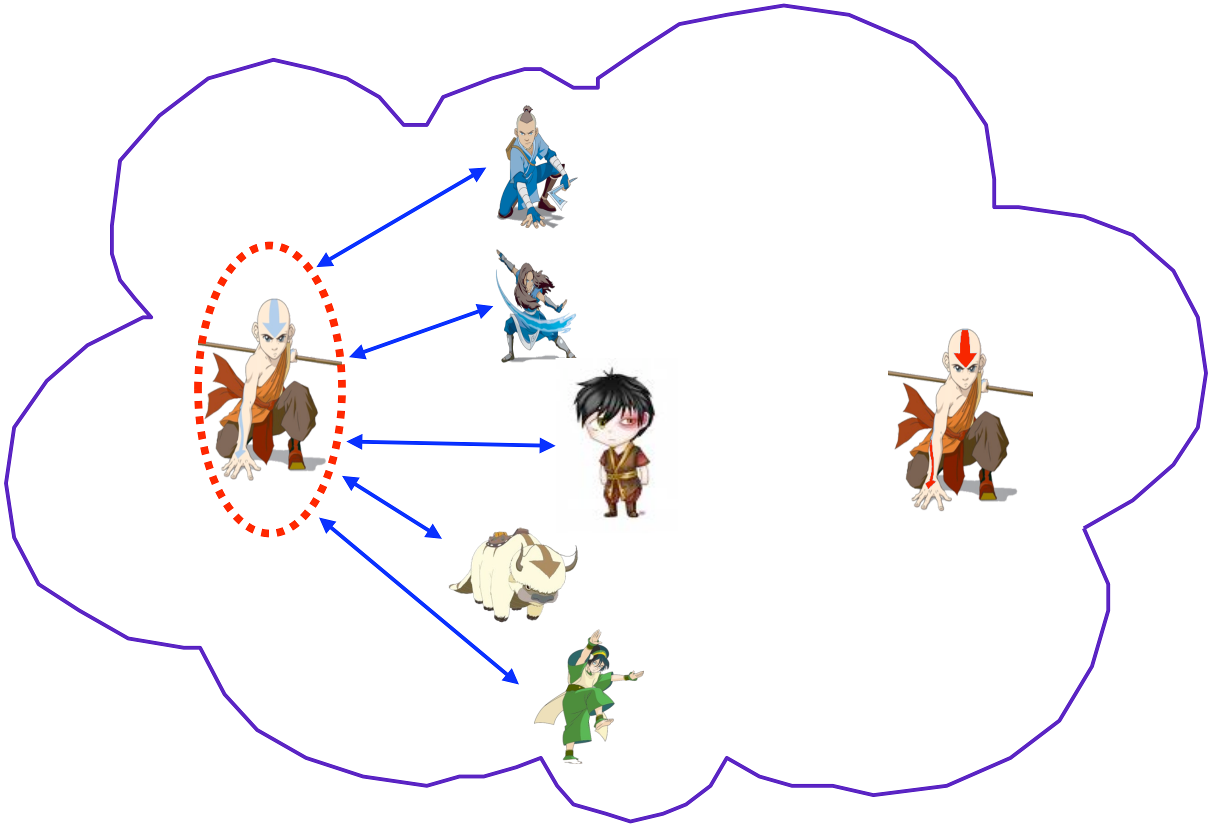
Status: Pending

Kristin Franceschi has indicated you are a Classmate at The Johns Hopkins University:

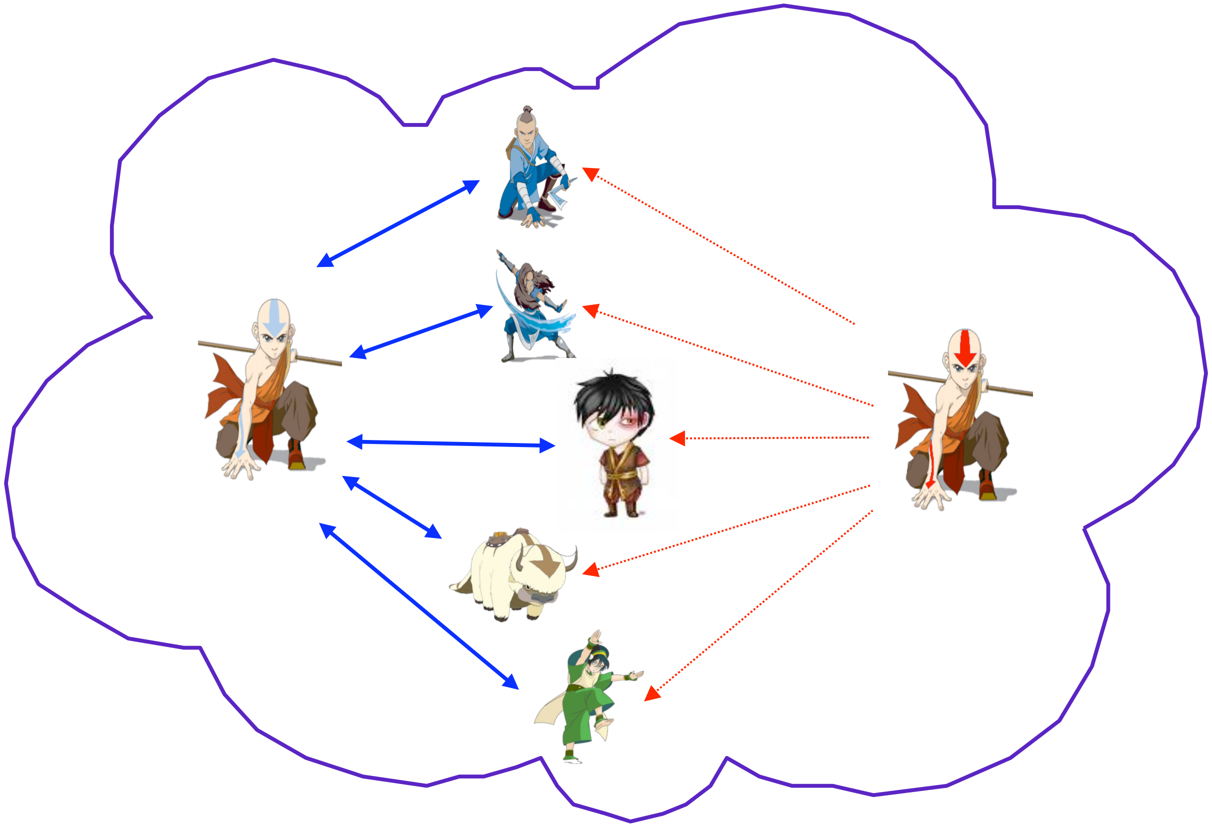
Whoa! You are there now! Can I be in your network?

Source: Shawn Moyer and Nathan Hamiel (BlackHat Talk)

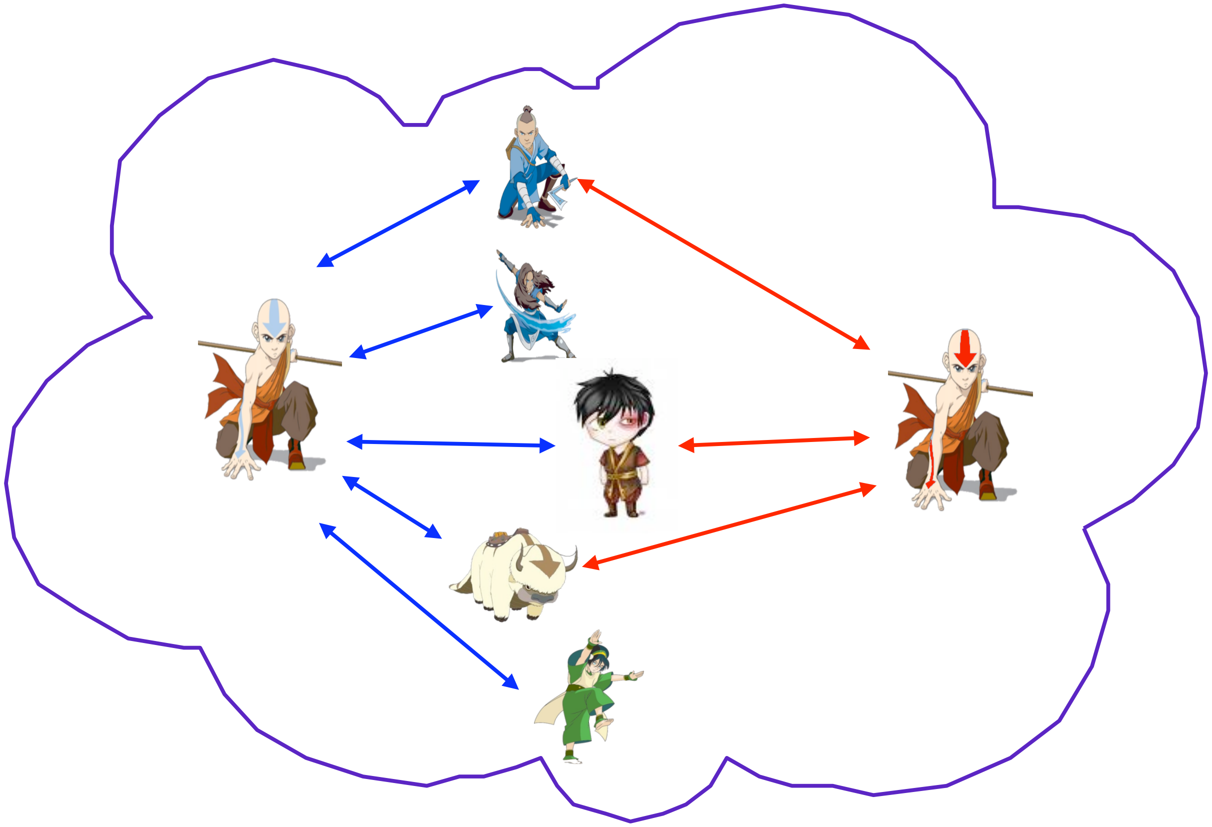
Profile Cloning



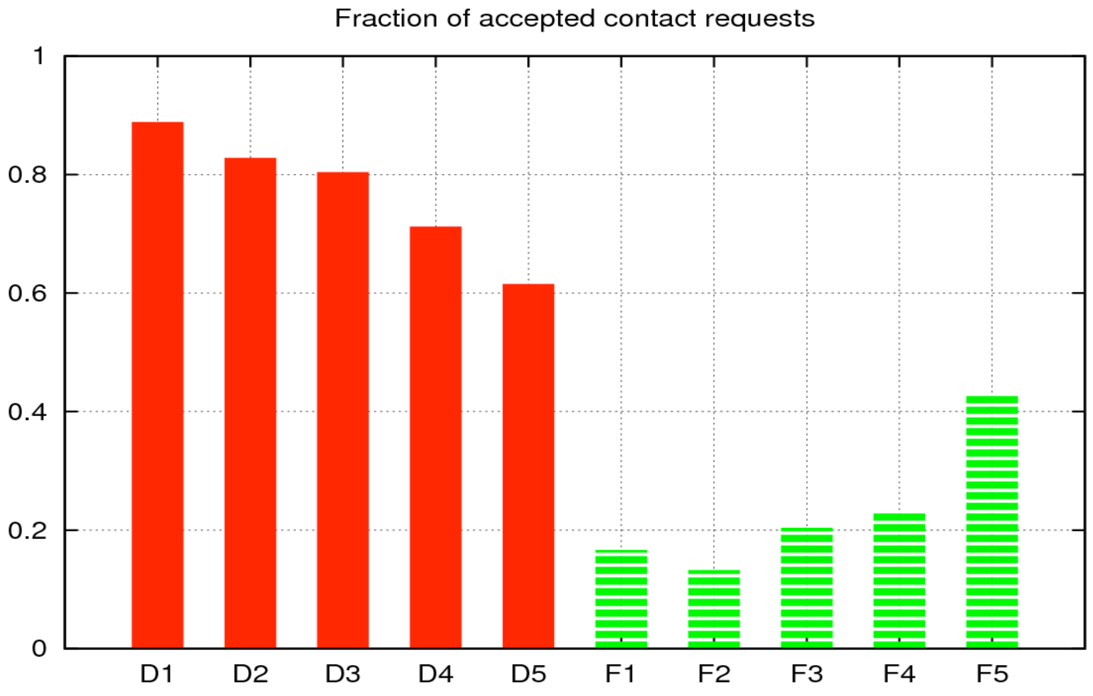
Profile Cloning



Profile Cloning

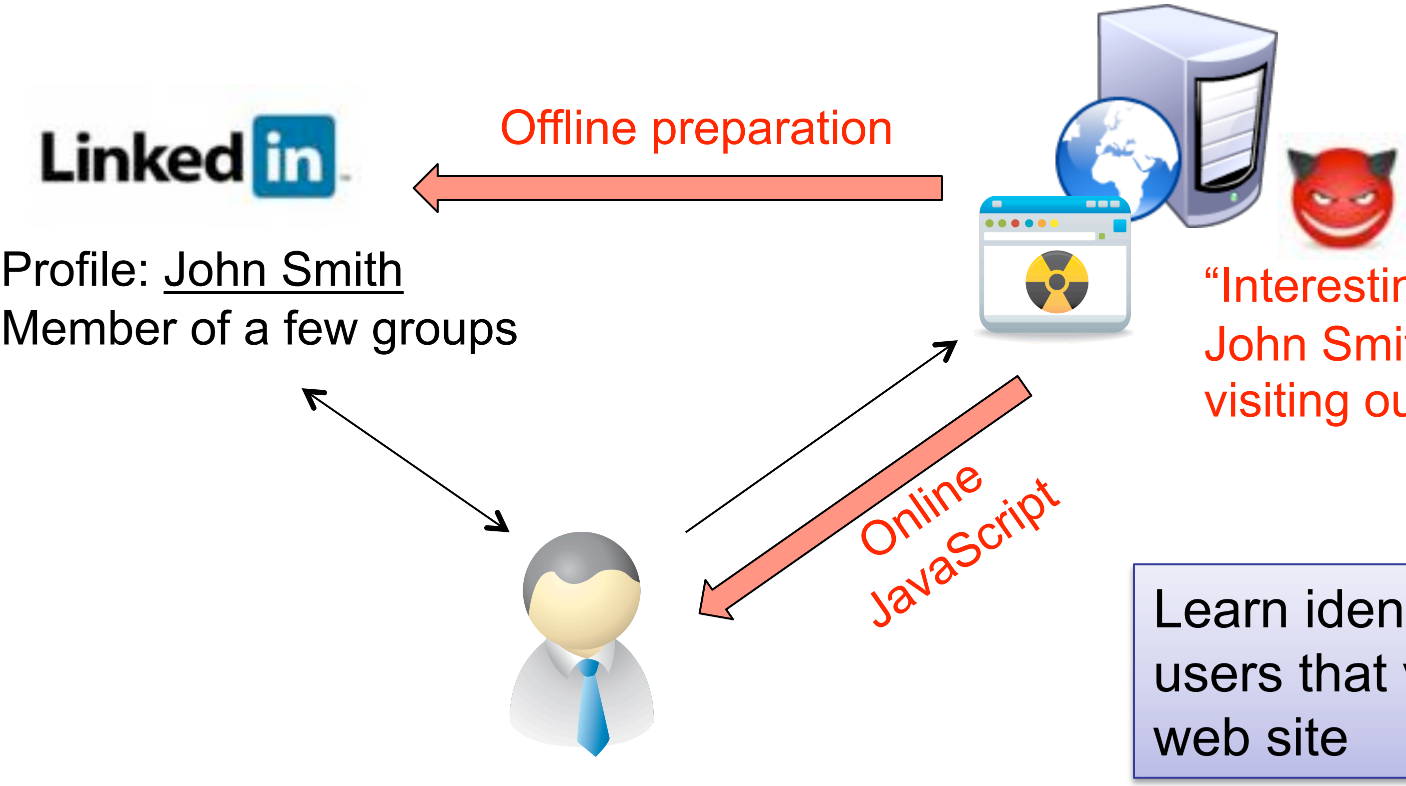


Profile Cloning



De-Anonymization of Third-Party Web Site Visitors

Attack Scenario



Offline preparation

Profile: John Smith
Member of a few groups

Online JavaScript

“Interesting … John Smith is visiting our site”

Learn identity of users that visit your web site

Offline Preparation

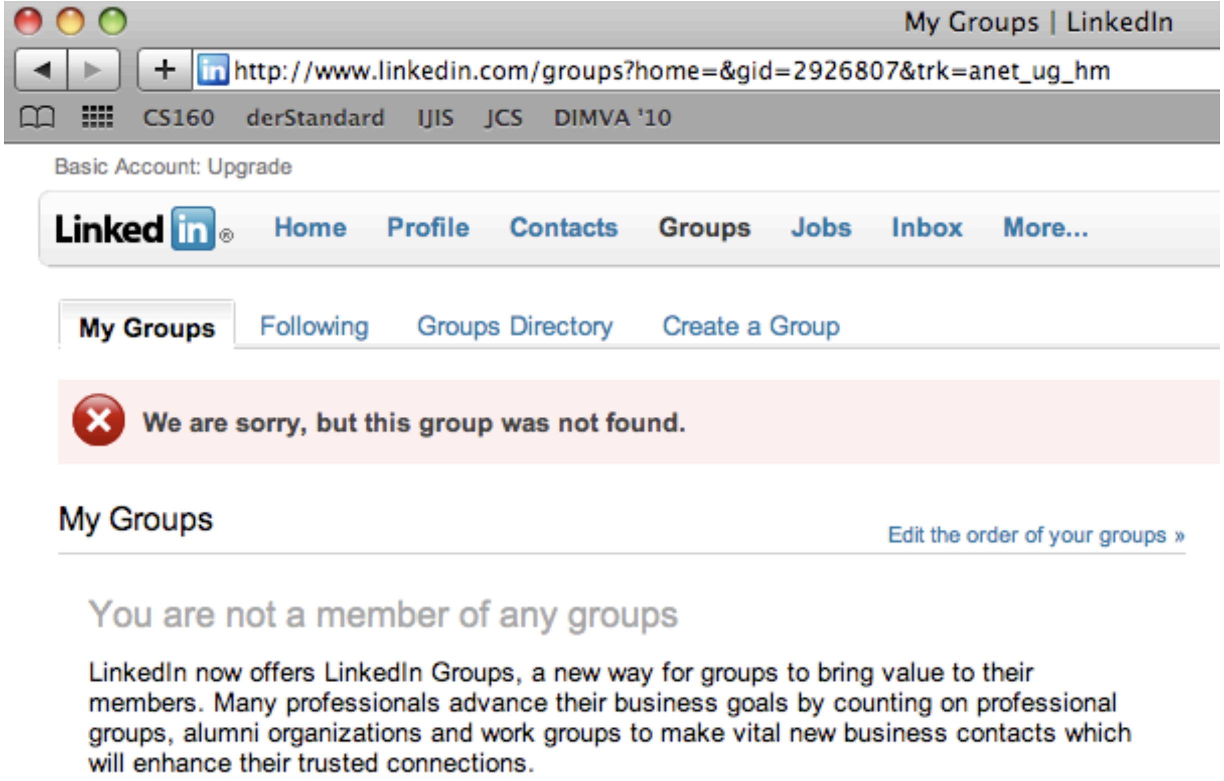
Learn group memberships of all social network users

- find all groups in social network
- determine members of each group

- Find groups
  - public group directories (Facebook)
  - predictable group identifiers (LinkedIn)

- Determine what users are members in a specific group
  - examine public group pages (Facebook)
  - join private group pages (more difficult)
  - examine user profiles (in LinkedIn, via public membership directory)

Finding Groups



We are sorry, but this group was not found.

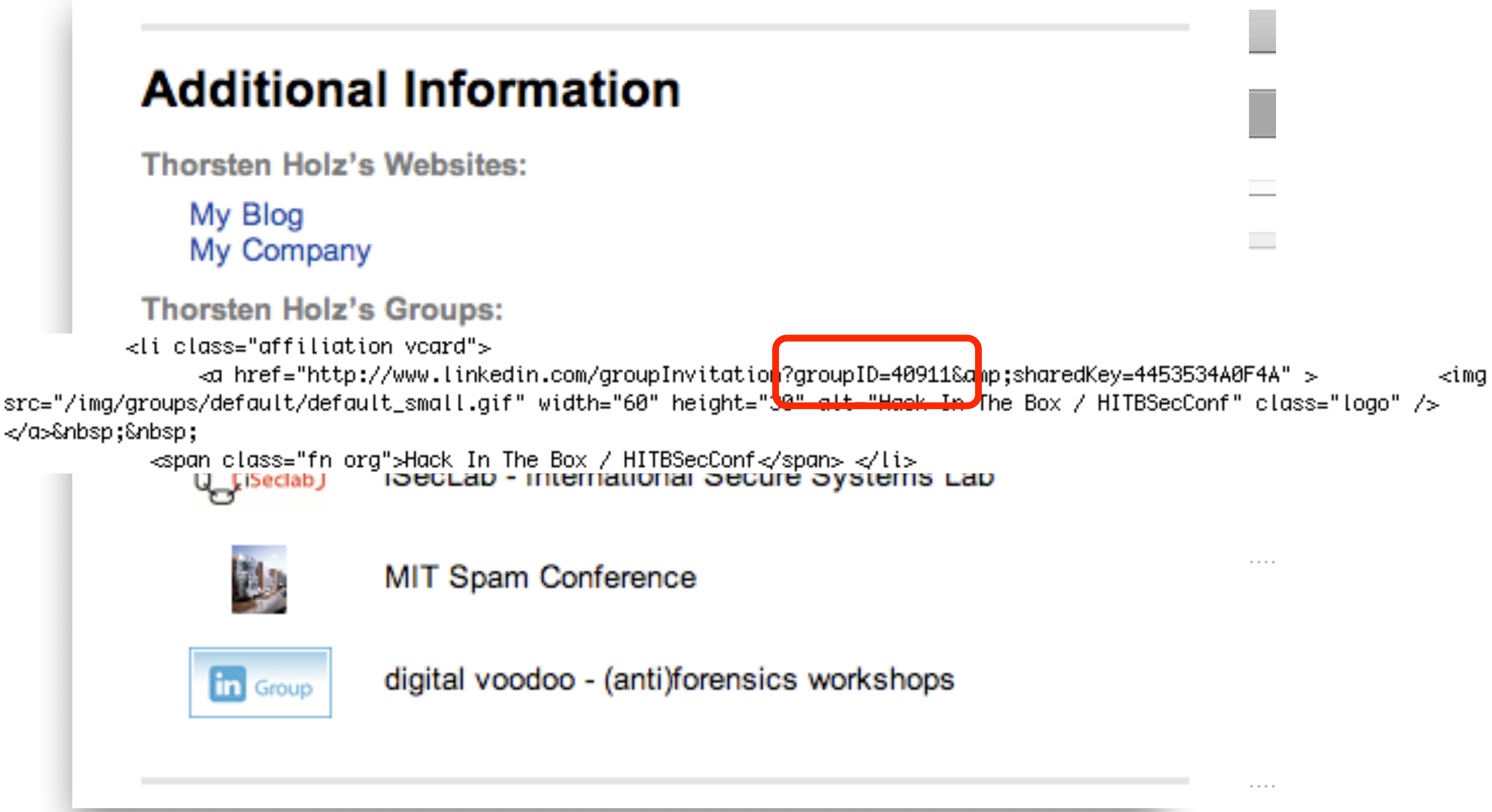
My Groups

Edit the order of your groups »

You are not a member of any groups

LinkedIn now offers LinkedIn Groups, a new way for groups to bring value to their members. Many professionals advance their business goals by counting on professional groups, alumni organizations and work groups to make vital new business contacts which will enhance their trusted connections.

Finding Membership Information



Additional Information

Thorsten Holz's Websites:

My Blog
My Company

Thorsten Holz's Groups:

```
        <li class="affiliation vcard">
                <a href="http://www.linkedin.com/groupInvitation?groupID=40911&amp;sharedKey=4453534A0F4A" >            <img
src="/img/groups/default/default_small.gif" width="60" height="30" alt="Hack In The Box / HITBSecConf" class="logo" />
</a>&nbsp;&nbsp;
          <span class="fn org">Hack In The Box / HITBSecConf</span> </li>
```

iSecLab - International Secure Systems Lab

MIT Spam Conference

digital voodoo - (anti)forensics workshops

Finding Membership Information

- Is it feasible?
  - we used 80legs service to crawl 3M LinkedIn group IDs for $7.49
  - randomly crawled 3M user profiles for $6.57
  - apologizes for wasting your resources
  - fully enumerated group memberships for Xing (8M users)

Online JavaScript Attack

- We now have group membership information, but …
  who cares?

<u>In the online part of the attack</u>

1. We leverage browser history stealing and predictable URLs
   to determine the groups that visitor is member of

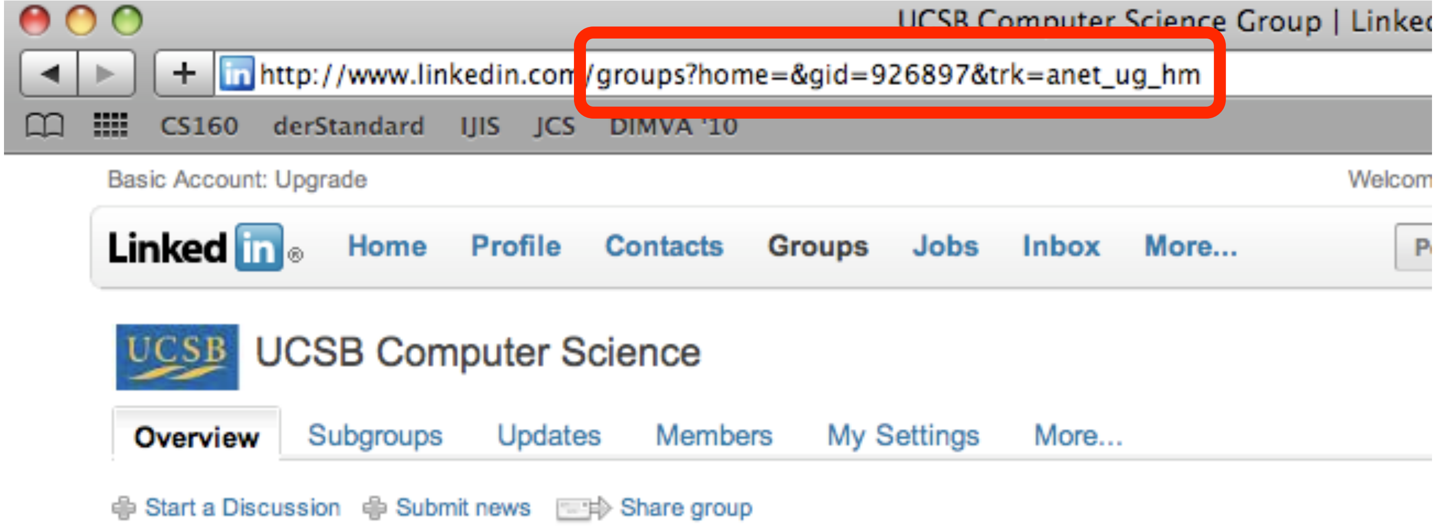
2. We combine this information with the group membership information
   to determine the identity of the visitor

Online Attack

- How does browser history stealing work?
  - well-known browser “problem” (typically considered harmless)
  - put a (hidden) link on a page and check its color (using CSS magic)
  - when link has been visited (i.e., it is in the browser history), then the color is different
  - serves as an oracle for presence / absence of specific URLs
  - note that you cannot simply read out entire history of the browser
  - our JavaScript sent to victim performs history stealing, that is, it checks for certain URLs

Online Attack

- Which URLs are checked?
  - those that indicate that a visitor is member of a group
  - this only works when such URLs exist and are predictable
  - fortunately (for the attacker), this is the case for most SNs



Candidate Sets

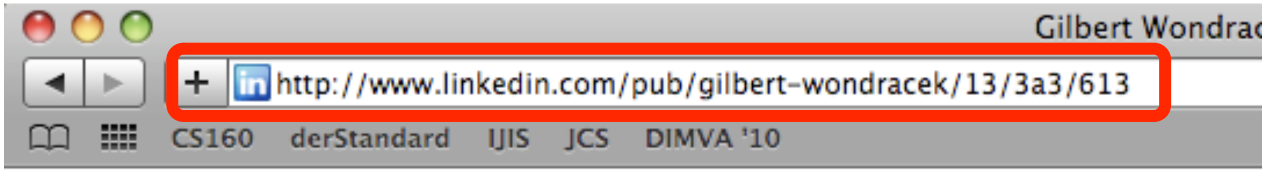
- In the best of all cases
  1. attacker obtains group memberships from history stealing
  2. intersects the known members in all these groups
  3. only one profile remains, and the person is de-anonymized

- But wait …
  - group memberships are not always unique, are they?
  - what happens when history stealing attack misses groups?

Candidate Sets

- Candidate sets
  - all users in intersection (or union) of identified groups
  - additional refinement step

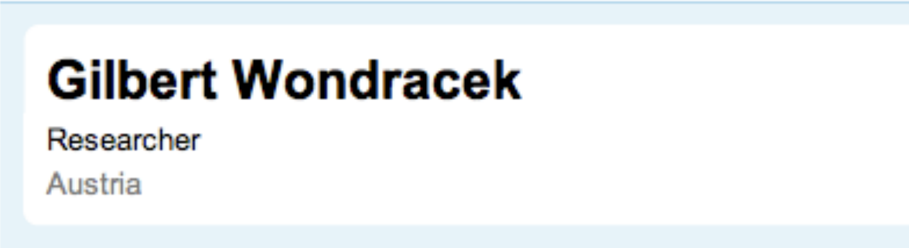
- Refinement step



Gilbert Wondrac

http://www.linkedin.com/pub/gilbert-wondracek/13/3a3/613

vay,



Gilbert Wondracek

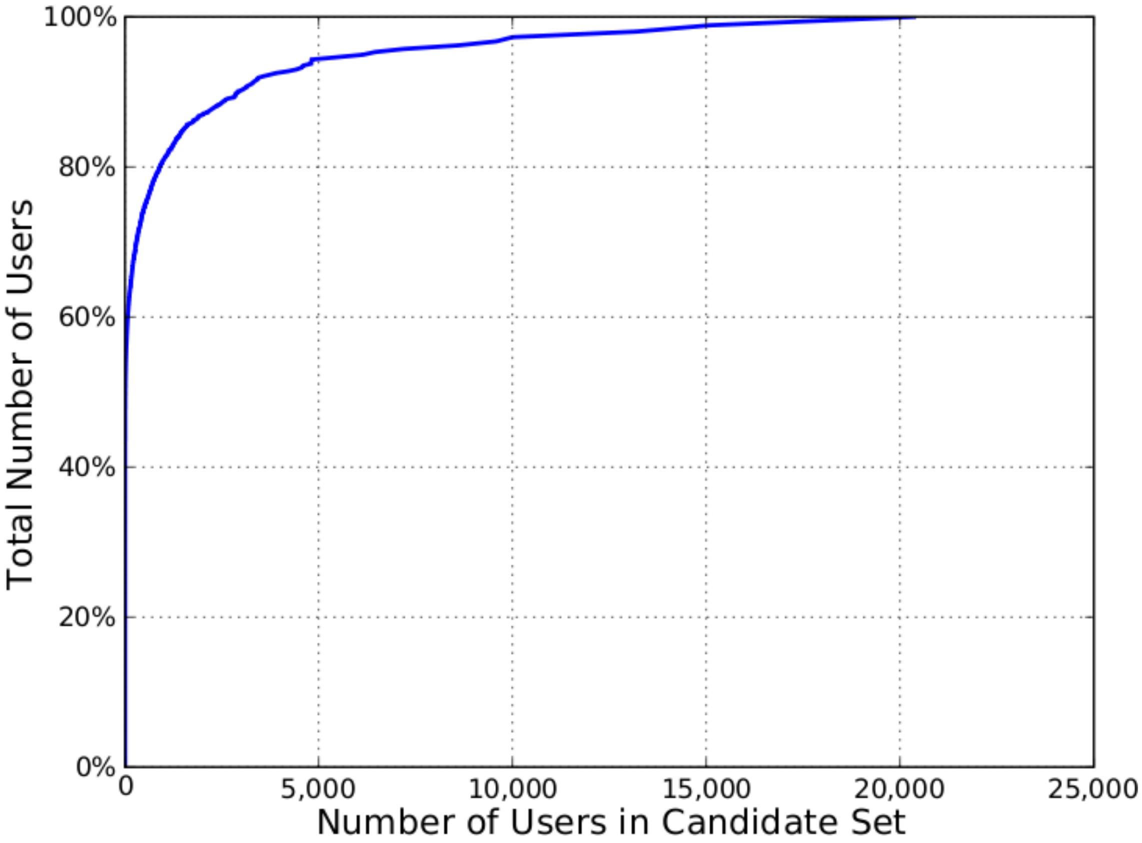
Researcher

Austria

Candidate Set Sizes

- Xing
  - 4.4 million membership relations, 1.8 million unique users in groups
  - 6,277 groups before the entire set of users is covered
  - 42.06% of users have a unique group fingerprint
  - for 90% of all users, the candidate set is < 2,912 users

Candidate Set Sizes



Experimental Evaluation

- Initial, small scale experiment on Xing
  - 15 out of 26 persons de-anonymized (they used Xing groups)
- Our findings got a lot of press, including links to experiment page
  - within a few days, thousands of users participated
- Results
  - 9,969 users finished the experiment
  - for 3,717 we found at least one group hit in browsing history (37,3%)
  - 1,207 (12,1%) regarded themselves as de-anonymized
- Of course, no ground truth about people who visited our site

Mitigation

- Make it hard for attacker to obtain group membership info

- Make it hard for attacker to predict group and user links
  - add random tokens to links (Xing)
  - use POST instead of GET (no parameters in URL)

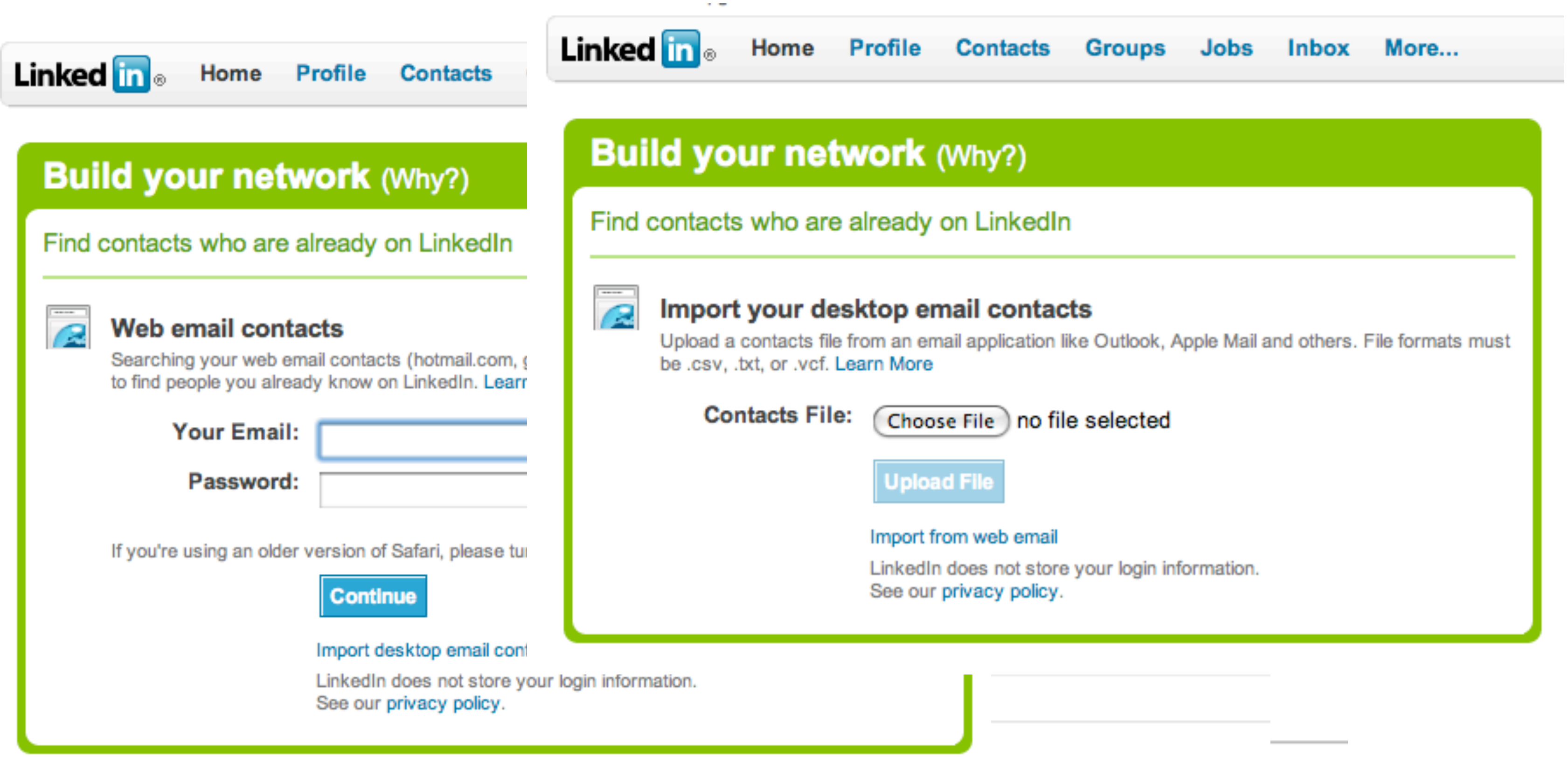
- Delete browser history
  - users can do this to protect themselves

- Fix history stealing attack

Abusing Friend Finder

Privacy Attacks

- Friend finder feature



Build your network (Why?)

Find contacts who are already on LinkedIn

Web email contacts

Searching your web email contacts (hotmail.com, g
to find people you already know on LinkedIn. Learn

Your Email:

Password:

If you're using an older version of Safari, please tu

Import desktop email cont

LinkedIn does not store your login information.
See our privacy policy.

Build your network (Why?)

Find contacts who are already on LinkedIn

Import your desktop email contacts

Upload a contacts file from an email application like Outlook, Apple Mail and others. File formats must be .csv, .txt, or .vcf. Learn More

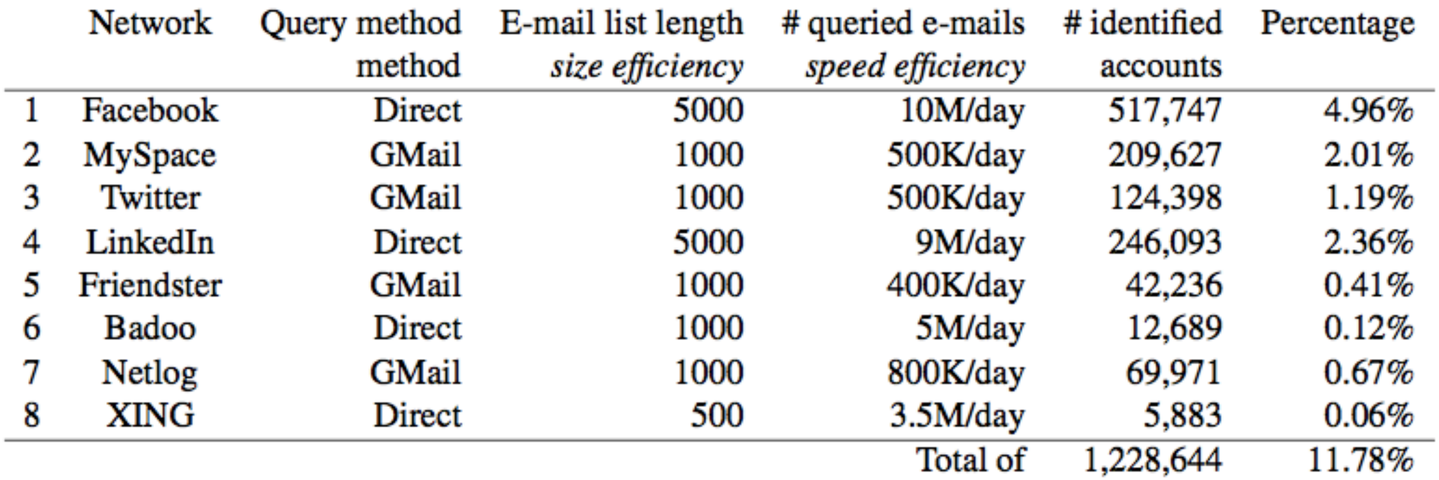
Contacts File: no file selected

Import from web email

LinkedIn does not store your login information.
See our privacy policy.

Privacy Attacks

- Abuse friend finder feature
  - in many networks, this feature is not protected (rate-limited)
  - allows millions of address queries in a short time (day)
  - oracle to check validity of mail addresses



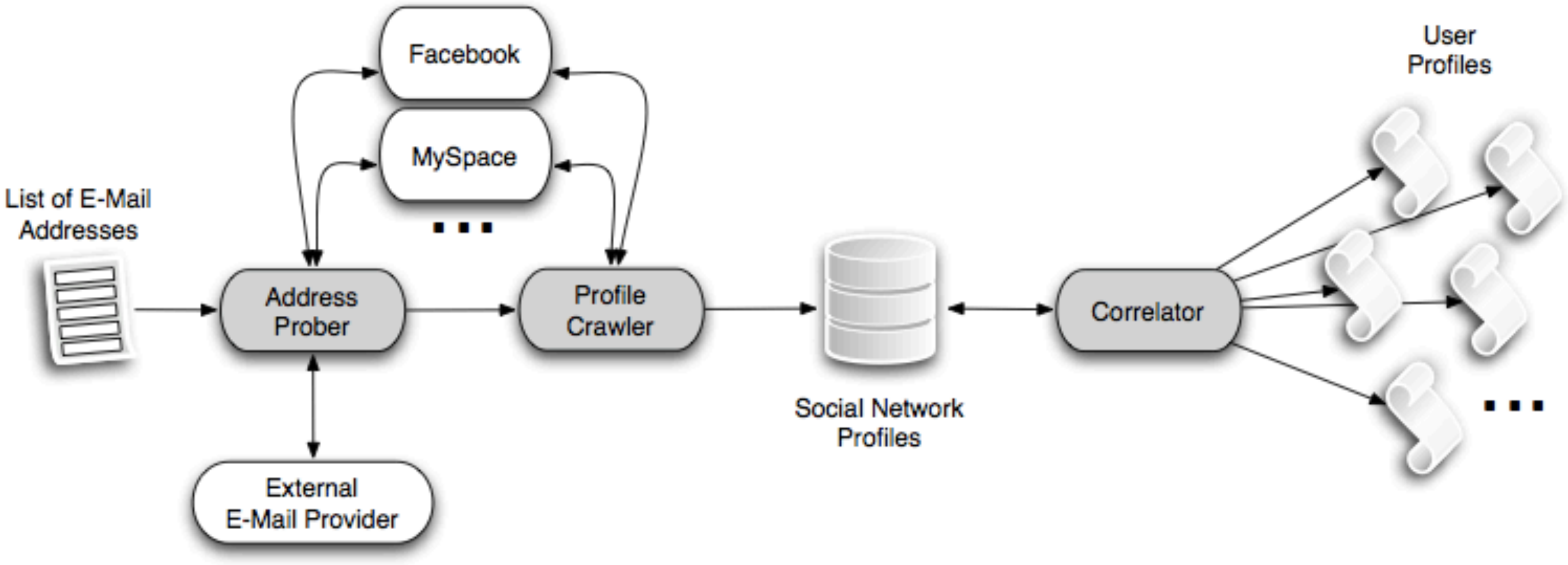
	Network	Query method method	E-mail list length *size efficiency*	# queried e-mails *speed efficiency*	# identified accounts	Percentage
1	Facebook	Direct	5000	10M/day	517,747	4.96%
2	MySpace	GMail	1000	500K/day	209,627	2.01%
3	Twitter	GMail	1000	500K/day	124,398	1.19%
4	LinkedIn	Direct	5000	9M/day	246,093	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	11.78%

Privacy Attacks

- Validate mail addresses as service for spammers
  - SMTP daemons have disabled this a long time ago
  - helpful also for spear phishing

- Connect profiles on different networks
  - aggregate information from different networks
  - but also reveals differences between peoples' identities
  - we found striking differences between profiles on professional networks (LinkedIn) and dating sites (Badoo)

Privacy Attacks



Mitigation

- Rate limiting
  - impose hard limits on email resolution –
    who is resolving more than X thousand mail addresses?
  - add CAPTCHAs to slow down attacker (Facebook)

- Limit amount of returned information
  - for example, do not link to actual profile

- Require names for each email address, and check for matches

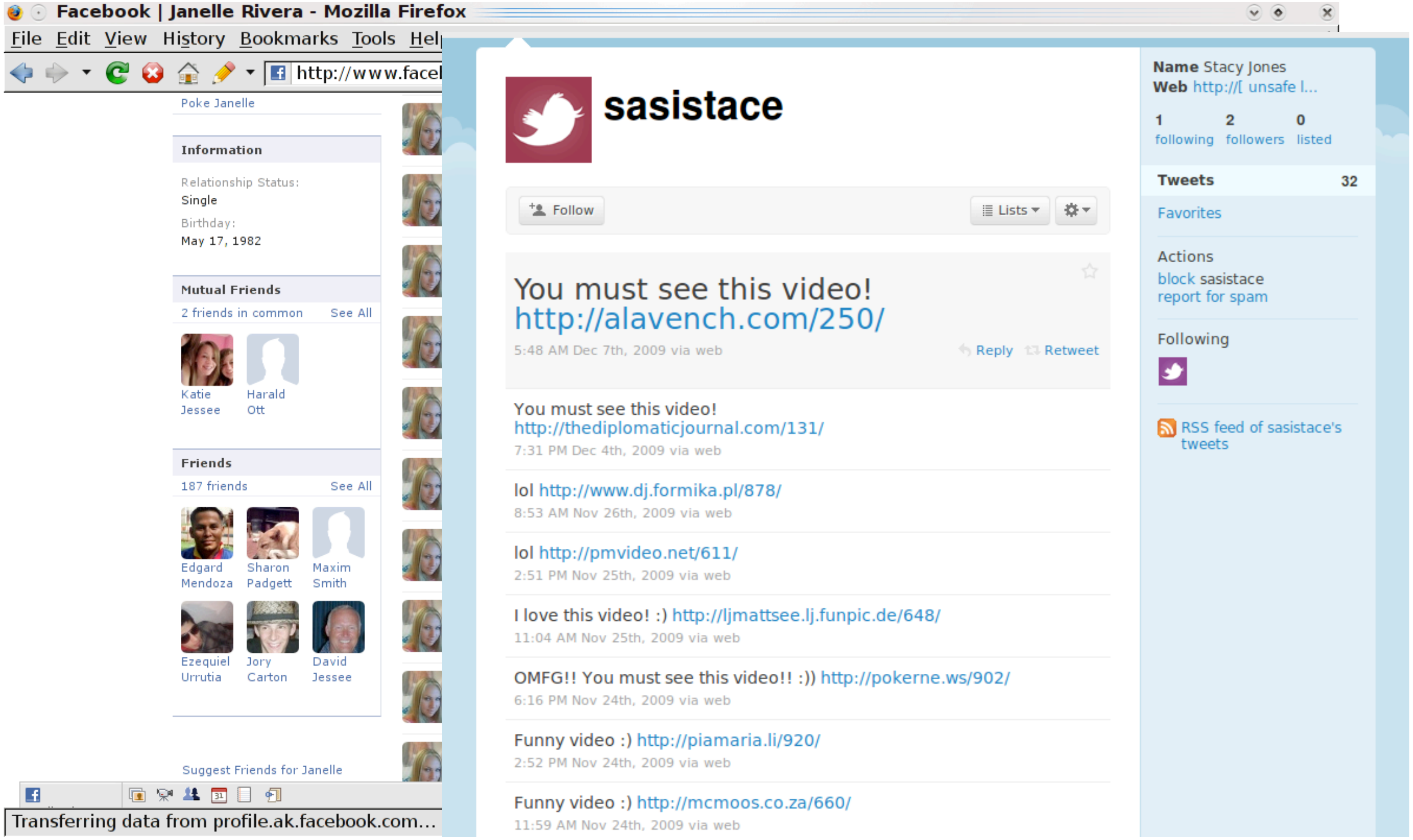
Social Network Security Issues

- Data privacy
  - blackmail
  - identity theft
  - personalized spear-phishing
  - targeted advertisement

- New venue to reach large number of potential victims
  - spam
  - malware / worms
  - links that point to sites with browser exploits (drive-by downloads)

Social Networking Spam

Spam on Social Networks



Facebook | Janelle Rivera - Mozilla Firefox

Information

Relationship Status:
Single
Birthday:
May 17, 1982

Mutual Friends

2 friends in common See All

Katie Jessee
Harald Ott

Friends

187 friends See All

Edgard Mendoza
Sharon Padgett
Maxim Smith
Ezequiel Urrutia
Jory Carton
David Jessee

Suggest Friends for Janelle

Transferring data from profile.ak.facebook.com...

sasistace

You must see this video! http://alavench.com/250/
5:48 AM Dec 7th, 2009 via web Reply Retweet

You must see this video! http://thediplomaticjournal.com/131/
7:31 PM Dec 4th, 2009 via web

lol http://www.dj.formika.pl/878/
8:53 AM Nov 26th, 2009 via web

lol http://pmvideo.net/611/
2:51 PM Nov 25th, 2009 via web

I love this video! :) http://ljmattsee.lj.funpic.de/648/
11:04 AM Nov 25th, 2009 via web

OMFG!! You must see this video!! :)) http://pokerne.ws/902/
6:16 PM Nov 24th, 2009 via web

Funny video :) http://piamaria.li/920/
2:52 PM Nov 24th, 2009 via web

Funny video :) http://mcmoos.co.za/660/
11:59 AM Nov 24th, 2009 via web

Name Stacy Jones
Web http://[unsafe l...

1 following 2 followers 0 listed

Tweets 32

Favorites

Actions
block sasistace
report for spam

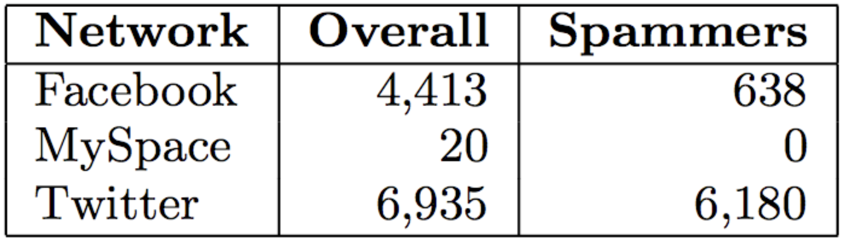
Following

RSS feed of sasistace's tweets

Spam Study

- Deployment of “honey” profiles
  - profiles that accept all friend requests
  - 300 profiles each on three networks (Facebook, MySpace, Twitter)
  - used different properties (to check for targeted campaigns)

- Findings
  - quite a bit of spam on Facebook and Twitter, little on MySpace



Network	Overall	Spammers
Facebook	4,413	638
MySpace	20	0
Twitter	6,935	6,180

Spam Study

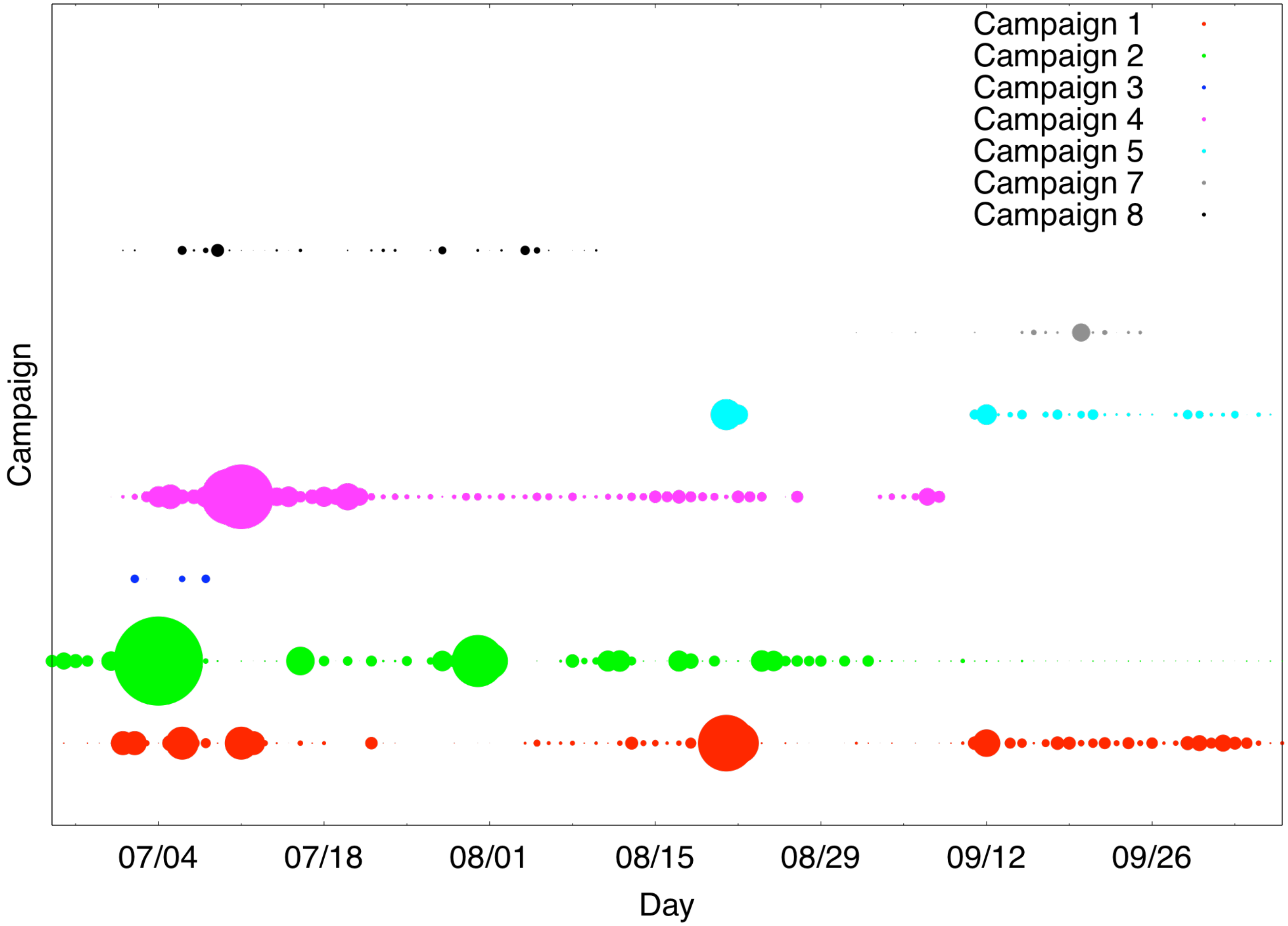
- Spam bots
  - template-based account generation
  - bots aggressively follow (connect to) other users

  - slow versus aggressive spamming (number of messages)
  - random versus targeted campaigns
    (we found a Facebook campaign that targeted male users)

  - messages share similarities
  - multiple bots operate in larger-scale campaigns

  - use “simple” interfaces (Twitter, Facebook mobile)

Spam Campaigns



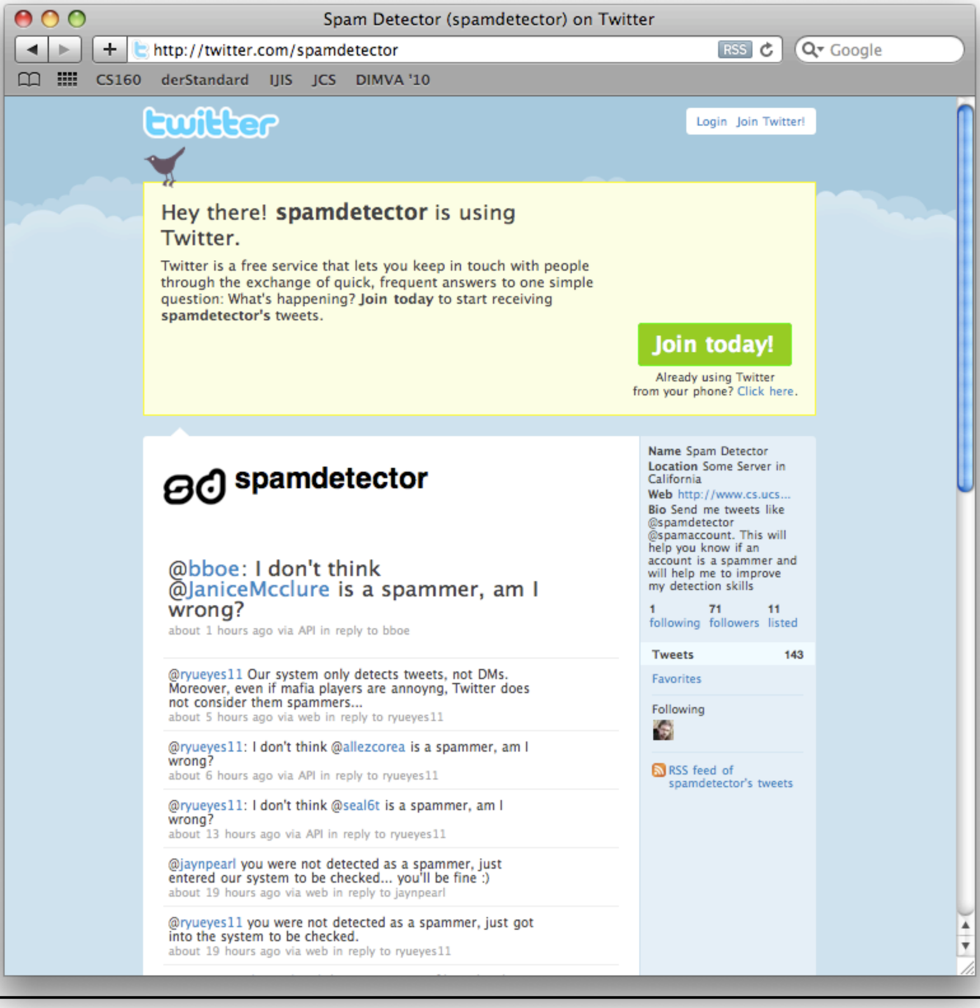
Spam Detection

- Leverage observations to build classifier (for Twitter)

- Features
  - following / followers ratio
  - URLs / message (tweets) ratio
  - message similarity
  - Twitter specific features:
    - retweet ratio, reply ratio, profile description presence

- Detection results
  - 13,258 spammers flagged and reported to Twitter
  - 62 false positives

Spam Detection Service


Spam Detector (spamdetector) on Twitter
http://twitter.com/spamdetector
RSS
Google
CS160
derStandard
IJIS
JCS
DIMVA '10
twitter
Login
Join Twitter!

Hey there! **spamdetector** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What's happening? **Join today** to start receiving **spamdetector's** tweets.

Join today!

Already using Twitter from your phone? Click here.

spamdetector

@bboe: I don't think @JaniceMcclure is a spammer, am I wrong?
about 1 hours ago via API in reply to bboe

@ryueyes11 Our system only detects tweets, not DMs. Moreover, even if mafia players are annoyng, Twitter does not consider them spammers...
about 5 hours ago via web in reply to ryueyes11

@ryueyes11: I don't think @allezcorea is a spammer, am I wrong?
about 6 hours ago via API in reply to ryueyes11

@ryueyes11: I don't think @seal6t is a spammer, am I wrong?
about 13 hours ago via API in reply to ryueyes11

@jaynpearl you were not detected as a spammer, just entered our system to be checked... you'll be fine :)
about 19 hours ago via web in reply to jaynpearl

@ryueyes11 you were not detected as a spammer, just got into the system to be checked.
about 19 hours ago via web in reply to ryueyes11

Name Spam Detector
Location Some Server in California
Web http://www.cs.ucs...
Bio Send me tweets like @spamdetector @spamaccount. This will help you know if an account is a spammer and will help me to improve my detection skills

1	71	11
following	followers	listed

Tweets 143

Favorites

Following

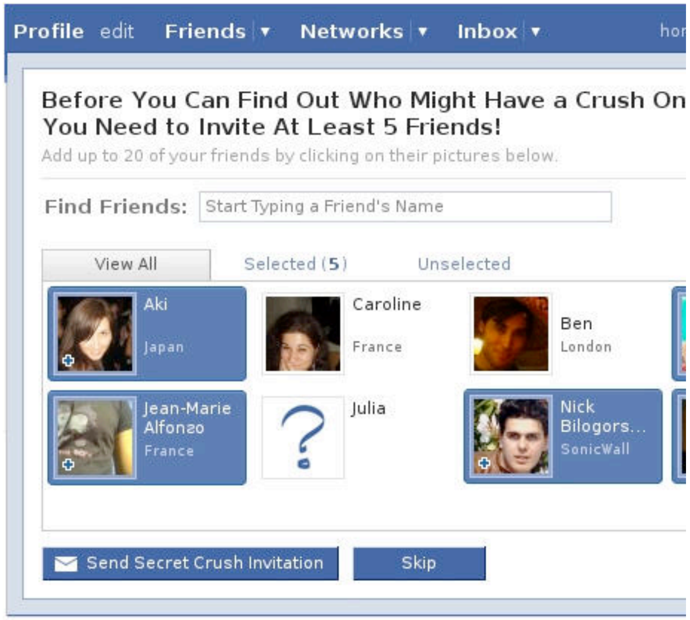
RSS feed of spamdetector's tweets

Malware and Worms

Famous Malware

- Samy (2005)
  - worm that attacked mySpace
  - exploited XSS vulnerabiity
- Orkut Worm (2007)
  - similar to Samy, but embedded Flash instead of JavaScript
- Secret Crush (2008)
  - leverages social engineering
  - links to download site for Adware
- Koobface (2009)
  - targets Facebook and several other social network sites
  - sends messages to friends of infected user, asks to download malware

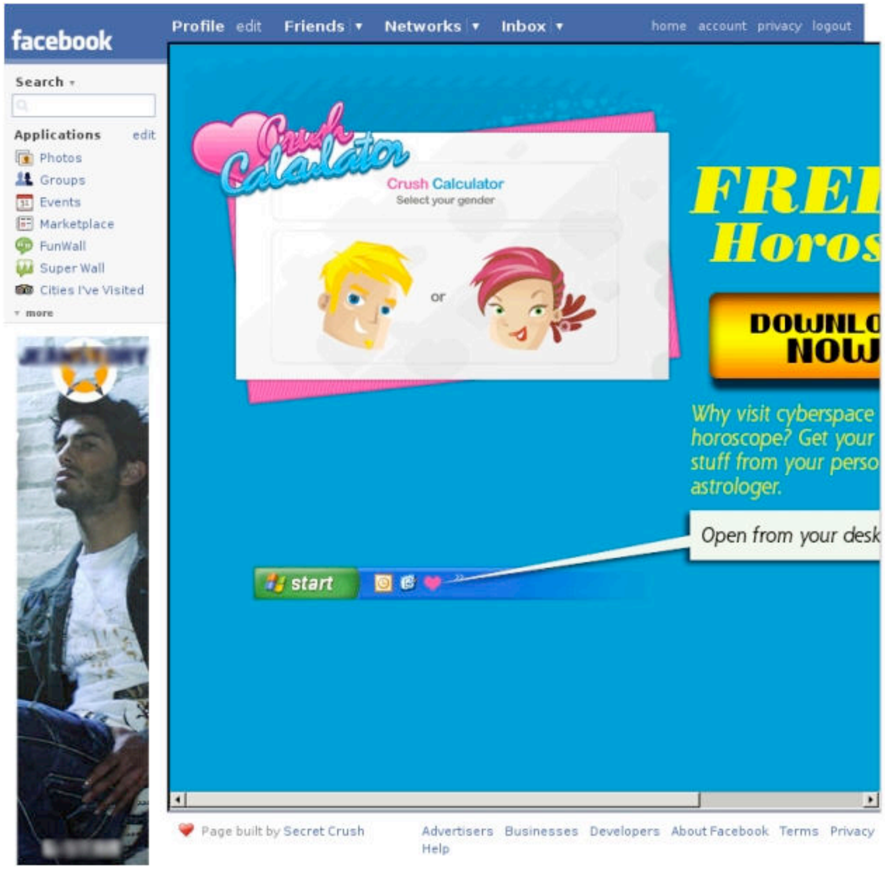
Secret Crush (2008)



Before You Can Find Out Who Might Have a Crush On You Need to Invite At Least 5 Friends!

Add up to 20 of your friends by clicking on their pictures below.

Find Friends: Start Typing a Friend's Name



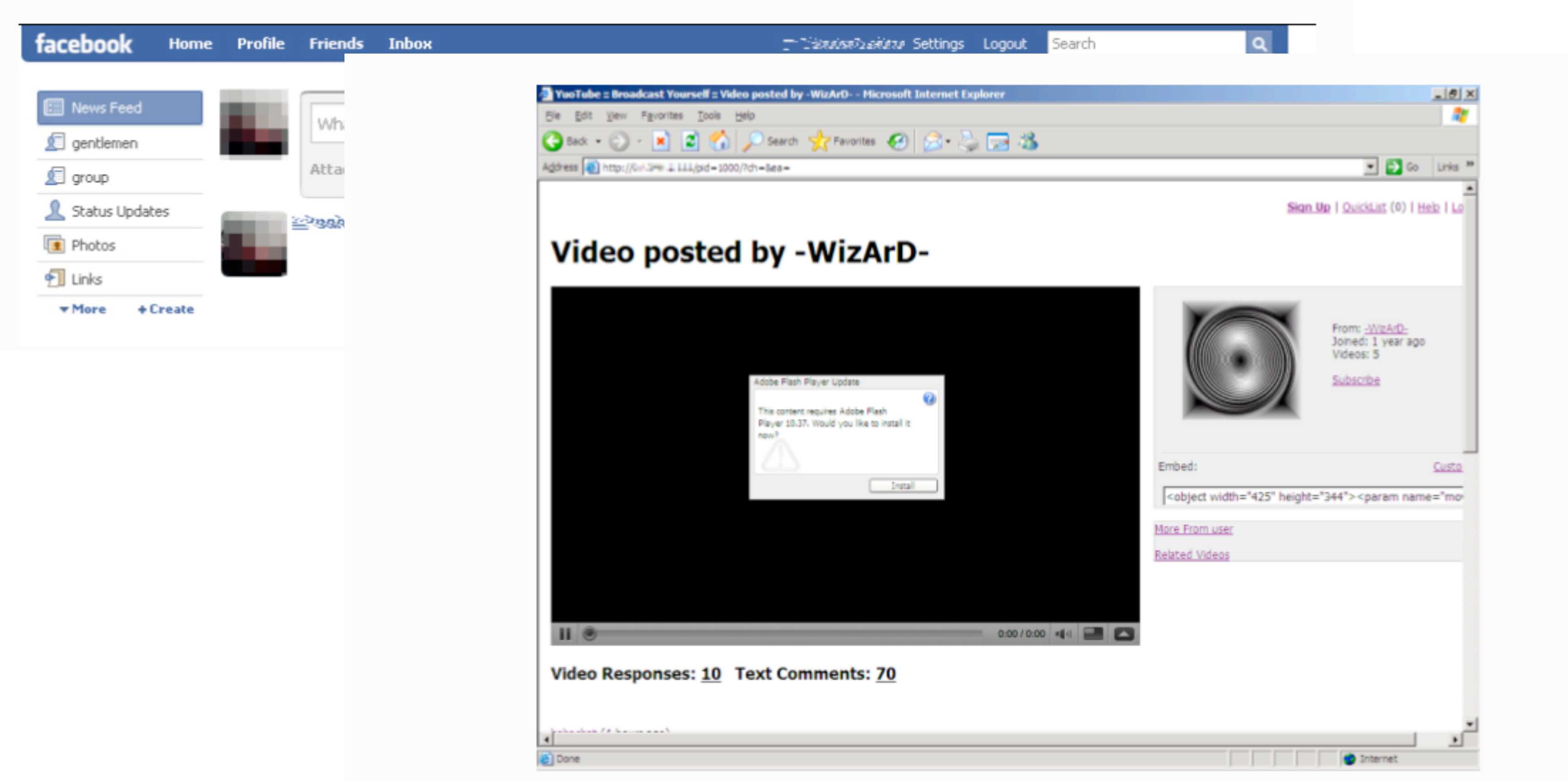
Why visit cyberspace horoscope? Get your stuff from your perso astrologer.

Open from your desk

Page built by Secret Crush

Figure 5: Zango IFrame

Koobface (2009)



Video posted by -WizArD-

This content requires Adobe Flash Player 10.37. Would you like to install it now?

<object width="425" height="344"><param name="mo

Video Responses: 10 Text Comments: 70

Figure 6. Copycat YouTube *site that leads to the KOOBFACE downloader*

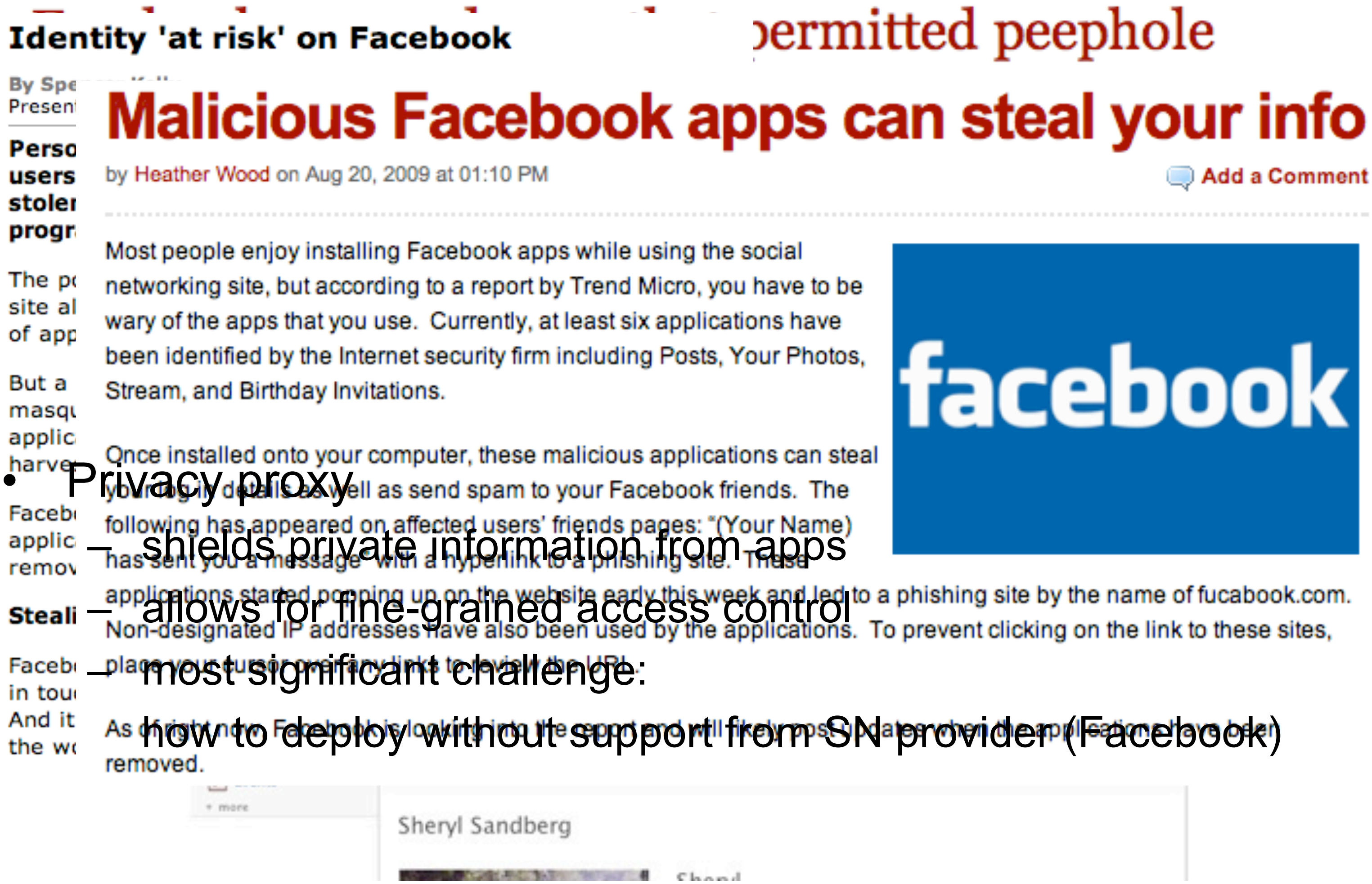
Social Network Security Issues

- Rogue applications
  - developed and under control of third parties
  - access to profile information and those of friends

- Support for regular crime
  - absence notes for burglary opportunities
  - monitor victim’s spending habits

- Crawlers
  - obtain large amount of data against will of social networks

Secure Third-Party Applications



Identity 'at risk' on Facebook

By Spe
Present

Perso
users
stoler
progr

The po
site al
of app

But a
masqu
applic
harve

Facebo
applic
remov

Steali

Facebo
in tou
And it
the wo

permitted peephole

Malicious Facebook apps can steal your info

by Heather Wood on Aug 20, 2009 at 01:10 PM

Add a Comment

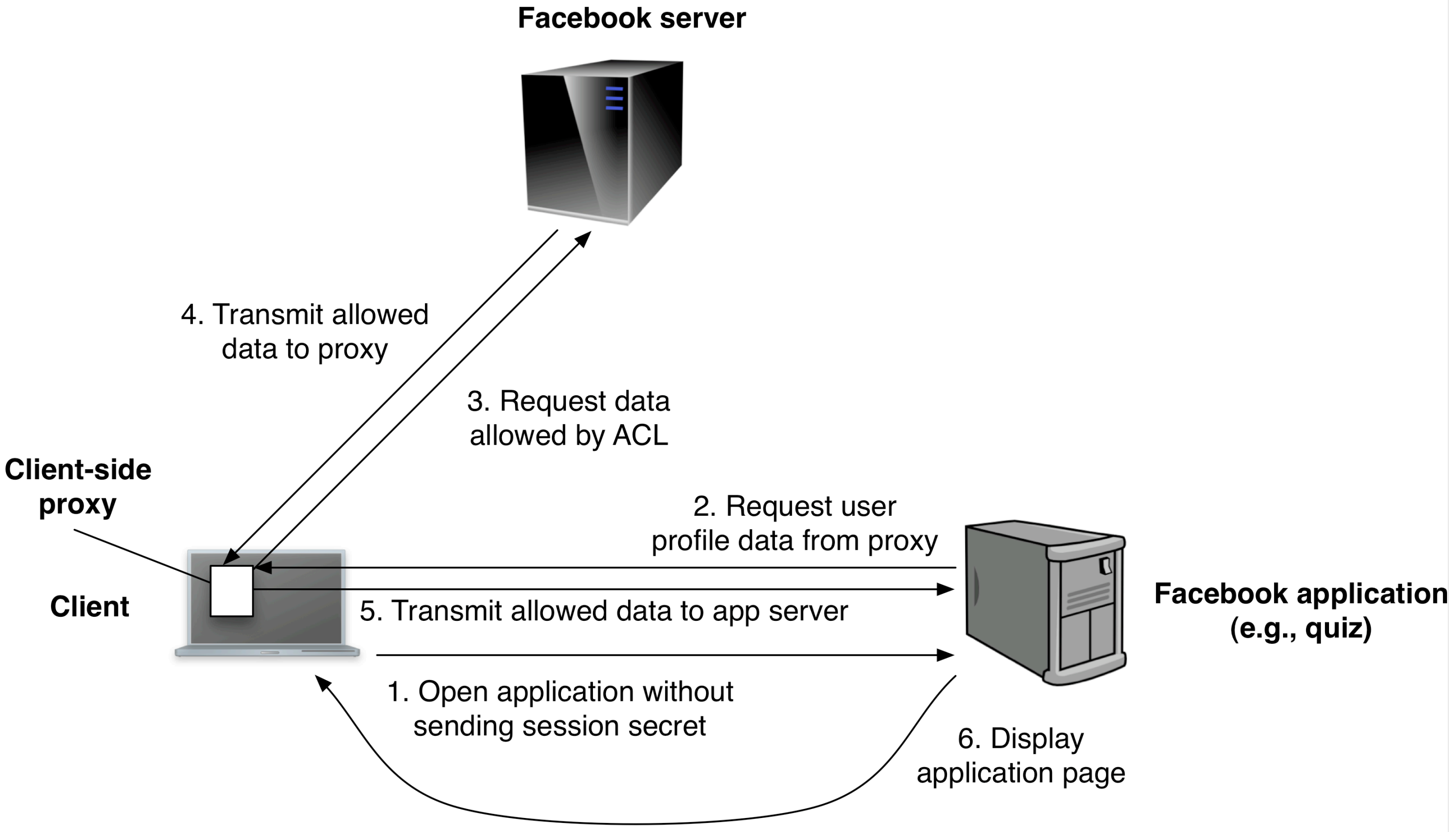
Most people enjoy installing Facebook apps while using the social networking site, but according to a report by Trend Micro, you have to be wary of the apps that you use. Currently, at least six applications have been identified by the Internet security firm including Posts, Your Photos, Stream, and Birthday Invitations.

Once installed onto your computer, these malicious applications can steal your login details as well as send spam to your Facebook friends. The following has appeared on affected users' friends pages: "(Your Name) has sent you a message" with a hyperlink to a phishing site. These applications started popping up on the website early this week and led to a phishing site by the name of fucabook.com. Non-designated IP addresses have also been used by the applications. To prevent clicking on the link to these sites, place your cursor over any links to view the URL.

As of right now Facebook is looking into the report and will likely post updates when the applications have been removed.

- Privacy proxy
  - shields private information from apps
  - allows for fine-grained access control
  - most significant challenge:
    - how to deploy without support from SN provider (Facebook)

Secure Facebook Applications



Facebook server
4. Transmit allowed data to proxy
3. Request data allowed by ACL
Client-side proxy
2. Request user profile data from proxy
Client
5. Transmit allowed data to app server
Facebook application (e.g., quiz)
1. Open application without sending session secret
6. Display application page

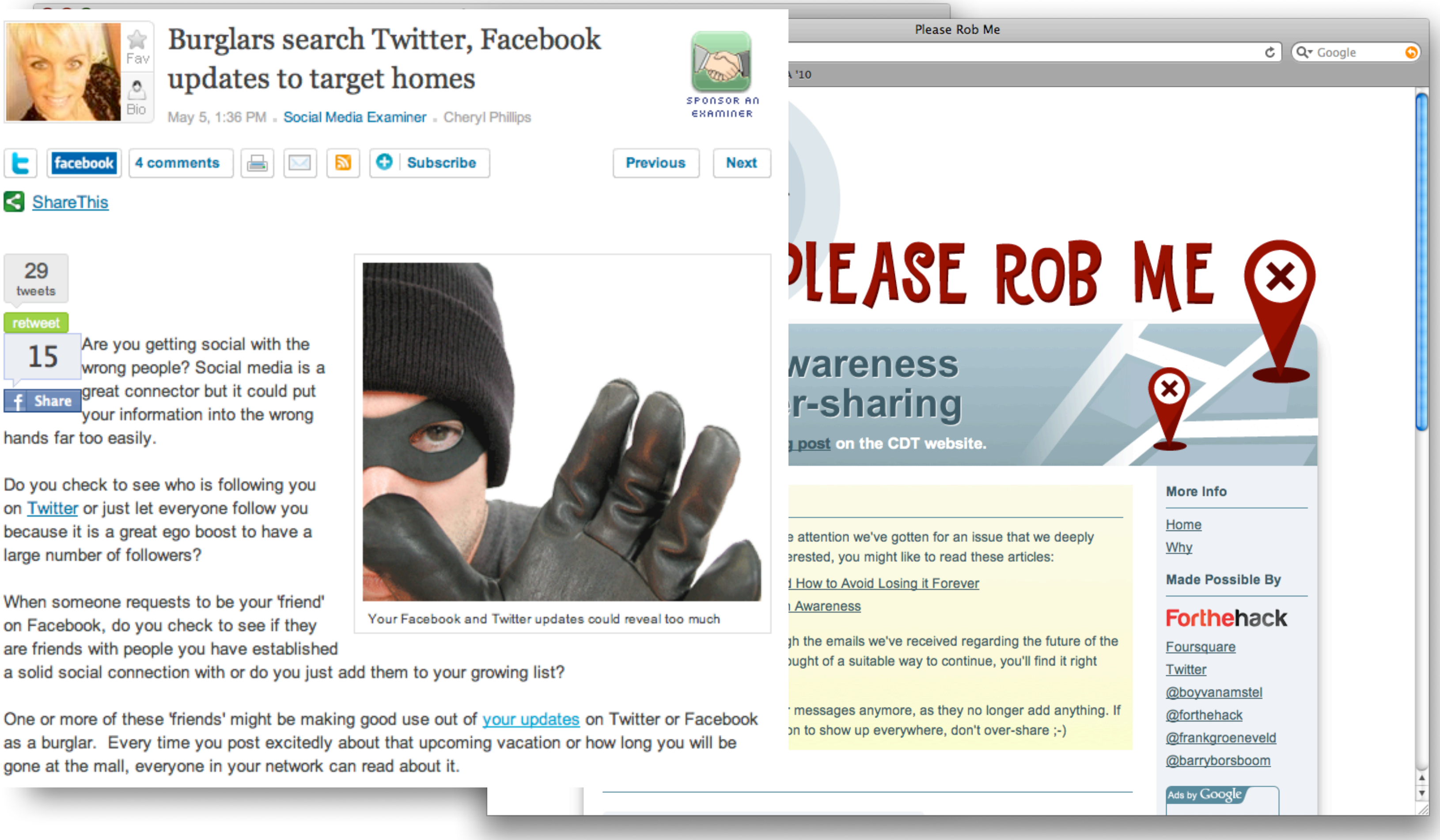
Social Network Security Issues

- Rogue applications
  - developed and under control of third parties
  - access to profile information and those of friends

- Support for regular crime
  - absence notes for burglary opportunities
  - monitor victim’s spending habits

- Crawlers
  - obtain large amount of data against will of social networks

Location-Based Services



Burglars search Twitter, Facebook updates to target homes

May 5, 1:36 PM . Social Media Examiner . Cheryl Phillips

Are you getting social with the wrong people? Social media is a great connector but it could put your information into the wrong hands far too easily.

Do you check to see who is following you on Twitter or just let everyone follow you because it is a great ego boost to have a large number of followers?

When someone requests to be your 'friend' on Facebook, do you check to see if they are friends with people you have established a solid social connection with or do you just add them to your growing list?

One or more of these 'friends' might be making good use out of your updates on Twitter or Facebook as a burglar. Every time you post excitedly about that upcoming vacation or how long you will be gone at the mall, everyone in your network can read about it.

Your Facebook and Twitter updates could reveal too much

g post on the CDT website.

e attention we've gotten for an issue that we deeply
erested, you might like to read these articles:

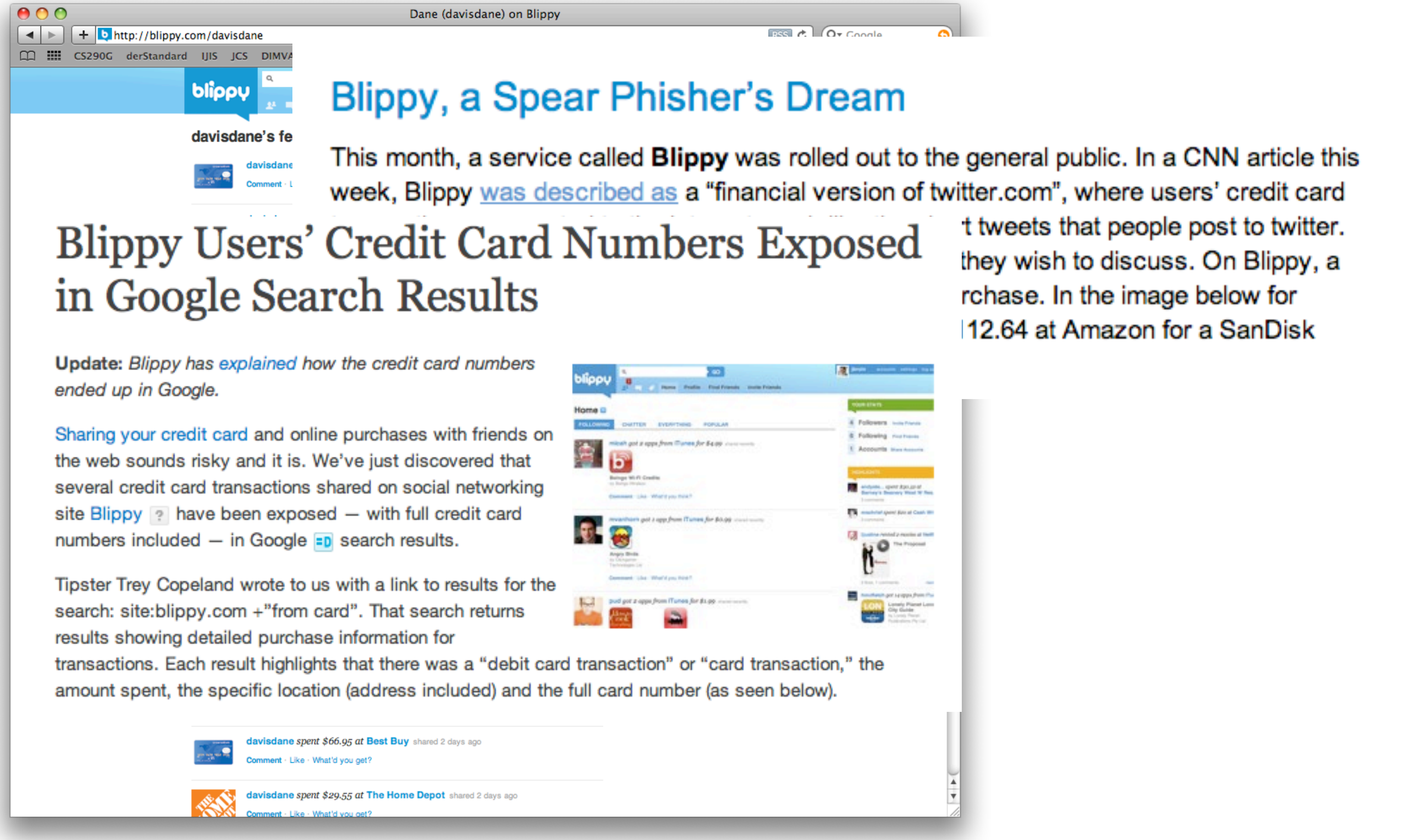
d How to Avoid Losing it Forever

n Awareness

gh the emails we've received regarding the future of the
ought of a suitable way to continue, you'll find it right

r messages anymore, as they no longer add anything. If
on to show up everywhere, don't over-share ;-)

Broadcast your Purchases



Dane (davisdane) on Blippy

http://blippy.com/davisdane

CS290G derStandard IJIS JCS DIMVA

davisdane's fe

davisdane

Comment · L

Blippy, a Spear Phisher's Dream

This month, a service called **Blippy** was rolled out to the general public. In a CNN article this week, Blippy was described as a "financial version of twitter.com", where users' credit card

't tweets that people post to twitter.

they wish to discuss. On Blippy, a

rchase. In the image below for

12.64 at Amazon for a SanDisk

Blippy Users' Credit Card Numbers Exposed in Google Search Results

Update: *Blippy has explained how the credit card numbers ended up in Google.*

Sharing your credit card and online purchases with friends on the web sounds risky and it is. We've just discovered that several credit card transactions shared on social networking site Blippy ? have been exposed — with full credit card numbers included — in Google search results.

Tipster Trey Copeland wrote to us with a link to results for the search: site:blippy.com +"from card". That search returns results showing detailed purchase information for transactions. Each result highlights that there was a "debit card transaction" or "card transaction," the amount spent, the specific location (address included) and the full card number (as seen below).

davisdane *spent $66.95 at* Best Buy shared 2 days ago

Comment · Like · What'd you get?

davisdane *spent $29.55 at* The Home Depot shared 2 days ago

Comment · Like · What'd you get?