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

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

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."
Data Privacy

• Wealth of sensitive and private information
  – not everything on Facebook is cool
  – so, how do social networks protect this data
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
Fake Profile (Ranum Experiment)

Source: Shawn Moyer and Nathan Hamiel (BlackHat Talk)
Profile Cloning
Profile Cloning
Profile Cloning
Profile Cloning

![Bar chart showing fraction of accepted contact requests]
De-Anonymization of Third-Party Web Site Visitors
Attack Scenario

Profile: John Smith
Member of a few groups

“Interesting … John Smith is visiting our site”

Learn identity of users that visit your web site

Offline preparation
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

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:**
- Hack In The Box / HITBSecConf
- 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?

In the online part of the attack

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
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
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
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

<table>
<thead>
<tr>
<th>Network</th>
<th>Query method method</th>
<th>E-mail list length size efficiency</th>
<th># queried e-mails speed efficiency</th>
<th># identified accounts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facebook</td>
<td>Direct</td>
<td>5000</td>
<td>10M/day</td>
<td>517,747</td>
</tr>
<tr>
<td>2</td>
<td>MySpace</td>
<td>GMail</td>
<td>1000</td>
<td>500K/day</td>
<td>209,627</td>
</tr>
<tr>
<td>3</td>
<td>Twitter</td>
<td>GMail</td>
<td>1000</td>
<td>500K/day</td>
<td>124,398</td>
</tr>
<tr>
<td>4</td>
<td>LinkedIn</td>
<td>Direct</td>
<td>5000</td>
<td>9M/day</td>
<td>246,093</td>
</tr>
<tr>
<td>5</td>
<td>Friendster</td>
<td>GMail</td>
<td>1000</td>
<td>400K/day</td>
<td>42,236</td>
</tr>
<tr>
<td>6</td>
<td>Badoo</td>
<td>Direct</td>
<td>1000</td>
<td>5M/day</td>
<td>12,689</td>
</tr>
<tr>
<td>7</td>
<td>Netlog</td>
<td>GMail</td>
<td>1000</td>
<td>800K/day</td>
<td>69,971</td>
</tr>
<tr>
<td>8</td>
<td>XING</td>
<td>Direct</td>
<td>500</td>
<td>3.5M/day</td>
<td>5,883</td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>Network</th>
<th>Overall</th>
<th>Spammers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>4,413</td>
<td>638</td>
</tr>
<tr>
<td>MySpace</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>Twitter</td>
<td>6,935</td>
<td>6,180</td>
</tr>
</tbody>
</table>
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

Campaign 1
Campaign 2
Campaign 3
Campaign 4
Campaign 5
Campaign 7
Campaign 8

Day

07/04 07/18 08/01 08/15 08/29 09/12 09/26
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

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.

@bboe: I don’t think @janiceMcclure is a spammer, am I wrong?

@nwyer: Our system only detects tweets, not DMs. Moreover, even if multi players are annoying, Twitter does not consider them spammers.

@nwyer: I don’t think @alesscoste is a spammer, am I wrong?

@nwyer: I don’t think @asell is a spammer, am I wrong?

@nwyer: You were not detected as a spammer, just enter our system to be checked... you’ll be fine.

@nwyer: You were not detected as a spammer, just enter our system to be checked.

Join today!
Malware and Worms
Famous Malware

- **Samy (2005)**
  - worm that attacked mySpace
  - exploited XSS vulnerability

- **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
Koobface (2009)

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

- Third-party applications are very powerful—especially on Facebook—all or nothing access to users' information—even a simple quiz can read all data (including those of friends)—power can be abused
- 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

1. Open application without sending session secret
2. Request user profile data from proxy
3. Request data allowed by ACL
4. Transmit allowed data to proxy
5. Transmit allowed data to app server
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, 136 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.
Broadcast your Purchases

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 tweets that people post to twitter, they wish to discuss. On Blippy, a purchase. In the image below for $12.84 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).