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
- Has > 800 Million active users
- The amount of personal information they store requires appropriate security precautions
- People are not aware of all the possible ways 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 …
And ...

### Find Friends

#### Add Personal Contacts as Friends

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Find Friends</td>
</tr>
<tr>
<td>2</td>
<td>Add Friends</td>
</tr>
<tr>
<td>3</td>
<td>Invite Friends</td>
</tr>
</tbody>
</table>

- **Windows Live Hotmail**
- **Windows Live Messenger**
- **orange.fr**
- **Yahoo!**
- **sfr.fr**
- **Other Email Service**

#### 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

xxxxemxy@gmxil.com;00000000;myrndejxx;Axxe Mxy
xxxxercxdxver@gmxil.com;00000000;megetxstic000;Megxn Ricxter
xxxxey0@xotmxil.com;00000000;Dopyy;Alixs Dykstrx
xxxxeydxe@gmxil.com;00000000;AntDrunk;Ant Brown
xxxxey.xudson@gmxil.com;00000000;Axxyeyxudson;Axxy Hudson
xxxxeylemieux00@xotmxil.com;00000000;xxxxylenieux;Axxy Lemieux
xxxxeylock@rogers.com;00000000;xxxxeylock;Joxnx Smetxust
xxxxeymorxn@gmxil.com;00000000;Axxtitx;0Axxy Morxn
xxxxie000@xotmxil.com;00000000;AxxieSmix00;Axxie Smix
xxxxie@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

<table>
<thead>
<tr>
<th>Network</th>
<th>Query method</th>
<th>E-mail list length</th>
<th># queried e-mails</th>
<th># identified accounts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>Direct</td>
<td>5000</td>
<td>10M/day</td>
<td>517,747</td>
<td>4.96%</td>
</tr>
<tr>
<td>MySpace</td>
<td>GMail</td>
<td>1000</td>
<td>500K/day</td>
<td>209,627</td>
<td>2.01%</td>
</tr>
<tr>
<td>Twitter</td>
<td>GMail</td>
<td>1000</td>
<td>500K/day</td>
<td>124,398</td>
<td>1.19%</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Direct</td>
<td>5000</td>
<td>9M/day</td>
<td>246,093</td>
<td>2.36%</td>
</tr>
<tr>
<td>Friendster</td>
<td>GMail</td>
<td>1000</td>
<td>400K/day</td>
<td>42,236</td>
<td>0.41%</td>
</tr>
<tr>
<td>Badoo</td>
<td>Direct</td>
<td>1000</td>
<td>5M/day</td>
<td>12,689</td>
<td>0.12%</td>
</tr>
<tr>
<td>Netlog</td>
<td>GMail</td>
<td>1000</td>
<td>800K/day</td>
<td>69,971</td>
<td>0.67%</td>
</tr>
<tr>
<td>XING</td>
<td>Direct</td>
<td>500</td>
<td>3.5M/day</td>
<td>5,883</td>
<td>0.06%</td>
</tr>
</tbody>
</table>

Total of 1,228,644
Extracted sensitive information

- Some statistics

<table>
<thead>
<tr>
<th>Platform</th>
<th>Age</th>
<th>Sex</th>
<th>Spoken Language</th>
<th>Job</th>
<th>Education</th>
<th>Current Relation</th>
<th>Searched Relation</th>
<th>Sexual Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>0.35</td>
<td>0.50</td>
<td>n/a</td>
<td>0.23</td>
<td>0.23</td>
<td>0.44</td>
<td>0.31</td>
<td>0.22</td>
</tr>
<tr>
<td>MySpace</td>
<td>82.20</td>
<td>64.87</td>
<td>n/a</td>
<td>3.08</td>
<td>2.72</td>
<td>8.41</td>
<td>4.20</td>
<td>4.07</td>
</tr>
<tr>
<td>Twitter</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>96.79</td>
<td>60.68</td>
<td>0.00</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Friendster</td>
<td>82.97</td>
<td>87.45</td>
<td>n/a</td>
<td>30.88</td>
<td>2.72</td>
<td>64.59</td>
<td>77.76</td>
<td>n/a</td>
</tr>
<tr>
<td>Badoo</td>
<td>98.61</td>
<td>98.61</td>
<td>47.81</td>
<td>17.06</td>
<td>19.92</td>
<td>22.48</td>
<td>n/a</td>
<td>22.80</td>
</tr>
<tr>
<td>Netlog</td>
<td>97.66</td>
<td>99.99</td>
<td>44.56</td>
<td>43.40</td>
<td>1.64</td>
<td>25.73</td>
<td>23.14</td>
<td>29.30</td>
</tr>
<tr>
<td>XING</td>
<td>n/a</td>
<td>n/a</td>
<td>84.54</td>
<td>99.87</td>
<td>49.21</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
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 `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

<table>
<thead>
<tr>
<th># SN</th>
<th># Profiles</th>
<th>Combination</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>608,989</td>
<td>Facebook - MySpace</td>
<td>57,696</td>
</tr>
<tr>
<td>2</td>
<td>199,161</td>
<td>Facebook - LinkedIn</td>
<td>49,613</td>
</tr>
<tr>
<td>3</td>
<td>55,660</td>
<td>Facebook - Twitter</td>
<td>25,759</td>
</tr>
<tr>
<td>4</td>
<td>11,483</td>
<td>Facebook - MySpace - Twitter</td>
<td>13,754</td>
</tr>
<tr>
<td>5</td>
<td>1,478</td>
<td>Facebook - LinkedIn - Twitter</td>
<td>13,733</td>
</tr>
<tr>
<td>6</td>
<td>159</td>
<td>Facebook - NetLOG</td>
<td>12,600</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>Badoo - FriendSter</td>
<td>11,299</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>Facebook - MySpace - LinkedIn</td>
<td>9,720</td>
</tr>
<tr>
<td></td>
<td>Total unique</td>
<td>LinkedIn - Twitter</td>
<td>8,802</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MySpace - Twitter</td>
<td>7,593</td>
</tr>
</tbody>
</table>
Information Mismatch

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

<table>
<thead>
<tr>
<th>Information</th>
<th>Value</th>
<th>% Total</th>
<th>% of mismatched values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>mismatches</td>
<td>2</td>
</tr>
<tr>
<td>Name</td>
<td>string</td>
<td>72.65</td>
<td>62.70</td>
</tr>
<tr>
<td>Location</td>
<td>city</td>
<td>53.27</td>
<td>51.74</td>
</tr>
<tr>
<td>Age</td>
<td>$0 &lt; n &lt; 100$</td>
<td>34.49</td>
<td>33.58</td>
</tr>
<tr>
<td>Sex</td>
<td>male, female</td>
<td>12.18</td>
<td>12.18</td>
</tr>
<tr>
<td>Sexual preference</td>
<td>straight, homosexual, bisexual</td>
<td>7.63</td>
<td>7.63</td>
</tr>
<tr>
<td>Current relationship</td>
<td>single, in a relationship, married, complicated</td>
<td>35.54</td>
<td>35.42</td>
</tr>
</tbody>
</table>
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
Chapter 2

Social engineering is the art of manipulating people 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
Too many connections.

Sorry, you cannot create any more connections.
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
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

Congratulations..............you are a beatiful and nice girl and I would 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
Kisses
Eric

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.

I dont 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 know 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 civic 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!

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
3 Types of Real-World RSE Attacks

- Recommendation-Based
  - Mediated attack where Recommendation System performs baiting
3 Types of Real-World RSE Attacks

- Demographic-Based – Mediated

- Visitor Tracking-Based – Direct
Experiment

- RSE attack on Facebook, Badoo and Friendster

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Facebook</th>
<th>Badoo</th>
<th>Friendster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommendation-Based</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demographic-Based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Visitor Tracking-Based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Determine characteristics which make profiles effective

<table>
<thead>
<tr>
<th>Social Network</th>
<th>Profile 1</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
<th>Profile 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>35</td>
<td>23</td>
</tr>
<tr>
<td>Sex</td>
<td>Male</td>
<td>Female</td>
<td>Female</td>
<td>Female</td>
<td>Female</td>
</tr>
<tr>
<td>Picture*</td>
<td><img src="image1.png" alt="Profile 1" /></td>
<td><img src="image2.png" alt="Profile 2" /></td>
<td><img src="image3.png" alt="Profile 3" /></td>
<td><img src="image4.png" alt="Profile 4" /></td>
<td><img src="image5.png" alt="Profile 5" /></td>
</tr>
</tbody>
</table>
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
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

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

Is this your intellectual property?

[Continue] [Cancel]
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 Very funny candid camera for a campaign against the abuse of alcohol :-)  
http://movie.ham-radio-op.net

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

```javascript
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

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Vulnerable</th>
<th>Patched</th>
<th>Not installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF</td>
<td>95</td>
<td>0</td>
<td>107</td>
</tr>
<tr>
<td>DIVX</td>
<td>7</td>
<td>5</td>
<td>190</td>
</tr>
<tr>
<td>FLASH</td>
<td>107</td>
<td>0</td>
<td>113</td>
</tr>
</tbody>
</table>
How do I spread an infection?
Clickjacking

- The classic Twitter example

```html
<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/amqzs6">
</iframe>

<button style="position: absolute; z-index: 1;">
Don’t Click
</button>
```
Likejacking

- Clickjacking applied to Social Networks
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
Chapter 5

- 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

Hop-by-hop privacy based on Node keys

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