

Security and Social Networking

Barry Leiba
Internet Messaging Technology

Aspects of Computer Security

- ◆ Authentication: Who am I? Prove it.
- ◆ Authorization: What am I allowed to do?
- ◆ Access Control: What can I allow others to do?
- ◆ Privacy: Am I safe from unauthorized viewing?
- ◆ Integrity: Am I safe from undetected changes?
- ◆ Non-repudiability: Can I or others deny what they said or did?

The Social Networking Model

- ◆ Everything is shared
- ◆ You make “friends”
- ◆ All friends are equal
- ◆ Some systems allow categorizing friends
 - ◆ It's not convenient
 - ◆ It's not really part of the model
- ◆ “Friending” is often fairly promiscuous
- ◆ Friends post public communiques to you

Some Problems

- ◆ IRL, not all friends are equal
 - ◆ You don't usually share everything with everyone
 - ◆ Close friends, work friends, ...
- ◆ IRL, it may not be easy to categorize friends
 - ◆ One friend belongs to multiple categories
 - ◆ The categories overlap in odd ways
 - ◆ Category combinations are unworkable

Some Problems

- ◆ IRL, you choose friends more carefully
 - ◆ Face-to-face information is more certain
 - ◆ Face-to-face interaction provides many cues
- ◆ IRL, your friends have more limited access
 - ◆ ...to you
 - ◆ ...to what you have to share
 - ◆ ...to your other friends
 - ◆ ...to what your other friends say

Example

- ◆ Joe has a party IRL
 - ◆ Some of Joe's friends are invited
 - ◆ Some are not
- ◆ The next day, friends post to Joe's "wall"
 - ◆ Thanks for the wonderful party!
 - ◆ What a great time we had!
 - ◆ Check out this pic from the party!
- ◆ Joe's uninvited friends see that too

Example

- ◆ *Is Britney Spears Spam?*
- ◆ Automated filtering in social networking?
- ◆ Much more a value judgment than with email
- ◆ You want to be her “friend”; I don't
- ◆ Is it really her?
- ◆ What are the tradeoffs?

Some Problems

- ◆ Online presence is vulnerable to malware
- ◆ Accepting certain things from false “friends” can be dangerous
- ◆ Once infected, you will infect real “friends”
 - ◆ ...even if they trust you

Example

- ◆ *Social Honeypots: Making Friends With A Spammer Near You*
- ◆ Researchers created MySpace identities
 - ◆ Waited for “friend” requests; stored and rejected
- ◆ 1570 requests, most within 2 months
 - ◆ Click traps, Friend infiltrators, Pornography, Pills
 - ◆ 1245 contained links
 - ◆ 1048 links worked
 - ◆ Only 6 unique clusters

Some Problems

- ◆ “Anonymized” data is aggregated for analysis
- ◆ Aggregated data is vulnerable (AOL problem)
- ◆ Anonymization isn't sufficient

Example

- ◆ *De-anonymizing Social Networks*
- ◆ Researchers looked at Flickr and Twitter
 - ◆ Anonymized network graph of Twitter
 - ◆ Identified network information from Flickr
- ◆ Relatively small overlap between the two
- ◆ Very successful at identifying Twitter users

Authentication & Access Control

- ◆ They like to use other services
 - ◆ Import your address book (from Gmail)
 - ◆ Access photos from Flickr (Yahoo!)
 - ◆ Print your friends' photos (Kodak Gallery)
- ◆ OpenID
 - ◆ Shared authentication service, no access control
- ◆ Oauth
 - ◆ Distributed access control
 - ◆ IETF chartering a working group

Legal Questions...

Is anonymization of data sufficient to protect our privacy?

As we live our lives more publicly, do we give up a legal sense of *expectation of privacy*?

References

- ♦ *Web Searchers' Identities Traced on AOL*; Barbaro, M. and T. Zeller Jr.; New York Times article; 9 August 2006;
<http://www.nytimes.com/2006/08/09/technology/08cnd-aol.html>
- ♦ *Is Britney Spears Spam?*; Zinman, A. & J. Donath; 4th Conference on Email and AntiSpam; August 2007; <http://www.ceas.cc/2007/papers/paper-82.pdf>
- ♦ *Social Honeypots: Making Friends With A Spammer Near You*; Webb, S., J. Caverlee, C. Pu; 5th Conference on Email and AntiSpam; August 2008;
<http://www.ceas.cc/2008/papers/ceas2008-paper-50.pdf>
- ♦ *De-anonymizing Social Networks*; Narayanan, A. and V. Shmatikov; IEEE Symposium on Security and Privacy; May 2009;
http://www.cs.utexas.edu/~shmat/shmat_oak09.pdf