CSE 543
Information Assurance and Security

Information Assurance in Social Computing

Professor Stephen S. Yau

What is Social Computing?

- **Social computing** is ***a collection of technologies*** supporting ***collaborative*** and ***interactive online social communications and related activities*** among users through ***online social networks*.**
- A ***social network*** is a ***social structure among social actors*,** such as individuals, groups, or organizations, which indicates ***specific types of social relationships or interdependencies*** in which the actors are connected.

Social Computing is Everywhere

- Social computing is not limited to certain social networking web sites.

Social Computing is Everywhere (cont.)

- Is one of most prevalent trends of applications on Internet
- Social computing technologies/applications are used everywhere on Internet
  - Emails
  - Blogs and forums
  - Wiki's / Twittering / Facebook / YouTube / Myspace,com
  - Instant messaging / Online chatting
  - Web 2.0 / peer to peer (P2P) networks
  - Voice communication / Video broadcasting / Photo sharing
  - Open source software development
  - Mobile / wireless computing
- The entire Internet itself is becoming a giant, interactive and powerful social network

Characteristics of Online Social Networks

- **User-created**
  - Regular websites are based on content updated by a webmaster and read by visitors.
  - Online social networks are ***built and updated by users***, populated with ***user-supplied contents***, such as conversations, photos, videos, scripts or articles.
  - Contents on online social networks become more diverse because
    - Users become more knowledgeable about social networks
    - Technologies enable broader connectivity (ubiquitous and pervasive)
    - PC and handheld devices become more powerful

Characteristics of Online Social Networks (cont.)

- ***Interactive***
  - Information flows in regular websites are unidirectional (from web servers to users), and future updates are determined by webmasters.
  - Information flows in online social networks are ***multi-directional*** (from web servers to users, from users to web servers, or from users to users), which make online social networks ***highly dynamic***.

Characteristics of Online Social Networks (cont.)

- ***Community-driven***
  - Online social networks are built and thrive from community concepts. Members of an online social network share ***commonalities***, such as beliefs, interests, hobbies, backgrounds, friendships, or jobs.
  - Online communities can be characterized by "***weak tie***" *
    - Easy to join and leave an online community
    - Members are loosely bounded (less reciprocal responsibilities among members).
    - Members can easily invite their friends to join their communities, and hence existing social networks can grow in term of size and richness of their contents

* Suarez, F. F. "Network Effects Revisited: The Role of Strong Ties in Technology Selection", *Academy of Management journal*, 48(4), 710–720, 2005.

Characteristics of Online Social Networks (cont.)

- ***Relationship-driven***
  - Highly diverse relationships among users, groups, organizations and communities.
  - Relationships among members are dynamically developed and changed.
  - More relationships you have with the members of a social network, more influence you are in the network
  - Two types of relationship
    - Direct relationship
    - Indirect relationship – e.g. friends of friends
  - Even if you have very few contacts with members, your publication may proliferate across the entire network through your contacts and their indirect contacts, which are much larger.

Characteristics of Online Social Networks (cont.)

- ***Heavily involving human factors***
  - Regular websites focus primarily on providing information to visitors
  - Online social networks contains a lot of contents involved with human behaviors and emotions, which may be difficult to predict
  - Many researchers try to study, analyze and simulate social behaviors of human via online social networks
    - Social network analysis has emerged as a key technique in sociology
    - Human behavior models (HBMs) and social network analysis are used in increasingly complex domains, such as military or manufacturing systems.

* E. Sabeur and G. Denis, "Human behavior and social network simulation: fuzzy sets/logic and agents-based approach", *Proc. 2007 Spring Simulation Multi-conference*, pp. 102-109

IA Issues on Online Social Networks

- Easy targets of cyber attacks
- Security and privacy issues
  - User management
  - Data management
  - Privacy management
  - Virus / worms / malicious scripts
  - Social engineering

User Management

- ***Difficult.***
  - Social networks involve ***unpredictable sets of participants***, including malicious users (hackers, private information collectors, phishers, or terrorists)
  - Users' memberships, roles and privileges are ***dynamically changed***
  - A user may have ***multiple identities*** for different social networks or communities
  - Establishing ***trustworthiness*** among users in a social network is difficult

User Management (cont.)

- What need to be done?
  - Proper digital identity management
  - Watch for anonymous access
  - Trust management
  - Efficient user authentication and authorization
  - Proper access control for dynamic user privileges
  - Detection of malicious behaviors

Data Management

- ***Difficult***
  - ***User-supplied data*** may violate laws or regulations
    - Violent/sexual contents, copyright-protected contents
  - ***Quality*** of user-supplied data is difficult to control
    - Anyone can publish his/her contents on social networks
    - Rumors / gossips / incitements / false information
  - ***Ownership*** of data is difficult to manage
    - Contents can be downloaded and republished on other social networks without owner's consent.
  - ***Integrity*** of data is difficult to protect
    - Contents can be downloaded and easily modified without owner's consent.

Data Management (cont.)

- What need to be done?
  - Efficient filtering for contents against laws or regulations
  - Efficient data quality control
    - A common way to control data quality in social networks is to use ***a reputation system***. A user's reputation is scored by other users' feedbacks on the content he/she published. (e.g. seller rating system of eBay)
  - Proper protection for copyrights and intellectual properties (e.g. digital watermarking)
  - Proper protection for data integrity (e.g. digital signature)

Privacy Management

- Two types of user-supplied content
  - ***Intentional content:*** Contents that users are willing to publish (e.g. blog posts, comments, reviews, ratings, links, RSS subscriptions, podcasts, and video).
  - ***Unintentional content:*** Byproducts of the intentional contents or the actions of users (e.g. metadata of intentional content, clickstreams, purchase history, search history, and other artifacts of behaviors).
- Privacy violation can occur on both intentional contents and unintentional contents

Privacy Management (cont.)

- Examples of privacy violation on ***intentional content*** in social networks.
  - A student lost a job offer after a recruiter finds pictures of him playing Beer Pong on his Facebook pages
  - A friend of mine downloaded my personal pictures and share them with other people I did not know
  - The system administrator sells personal data without permission

Privacy Management (cont.)

- Examples of privacy violation on ***unintentional content*** in social networks
  - A cell phone application reveals your location to your friends
  - A photographer published a set of photos, and the metadata of the photos contained information about GPS locations where he took the photos.
  - An employee posted unpleasant comments about his boss anonymously. However, the employee’s IP address was logged in the system log during the posting. Later, the boss found out who posted the comments by tracking IP address.

* S. Motahar et al, "Seven Privacy Worries in Ubiquitous Social Computing", *Proc. the 3rd Symposium on Usable Privacy and Security*, 2007, pp. 170-172

Privacy Management (cont.)

- What need to be done?
  - ***User-centric privacy management***
    - User has control over
      - Who can access my content
      - How my personal information is collected
      - What kinds of unintentional content will be generated
  - ***Fundamental principles for privacy protection***
    - ***Notify users*** regarding collection, use and disclosure of personally identifiable information (PII)
    - Provide users ***the choice to opt out or opt in*** regarding disclosure of PII to third parties
    - Provide users the ***security to protect PII*** from unauthorized access
    - ***Enforce*** applicable privacy policies, laws and regulations

Viruses, Worms and Malicious Scripts

- Online social networks are easy target of viruses, worms or malicious scripts
  - Malicious users can easily publish contents containing viruses, worms or malicious scripts (e.g. cross-site scripting) which can quickly propagate through the social networks.
- What need to be done?
  - Sanitizing/validating user-supplied data
  - Intrusion detection

Social Engineering

- ***Social Engineering*** (art of deception) is manipulating people by abusing social skills to obtain sensitive information http://www.us-cert.gov/cas/tips/ST04-014.html
  - Exploits human aspects of computing
  - One of hardest forms of attack to defend against because it cannot be prevented by technologies.
    - Human aspects are unpredictable.
    - The weakest link in any security scheme is ***the user***.
  - Example: The ILOVEYOU virus, discussed in Lecture 2, used social engineering – exploiting the weakness that curious people are likely to click on the email attachment.

Social Engineering (cont.)

- Social networks are vulnerable to social engineering because social networks are ***community-driven*** and ***relationship-driven***.
  - Malicious user can easily collect useful information about a victim from social networks for deceiving the victim. Such information includes name, age, job, interests, hobbies, family background and personality.
  - Data mining can be very useful for social engineering
  - If a malicious user successfully deceives a victim, the user may also easily deceive other users who have relationships with the victim on the social networks.

Social Engineering *(cont.)*

- Social engineering techniques
  - ***Impersonation*** – convincing a victim that the malicious user is someone he isn't
    - Example: A malicious user contacts a victim, claiming to be a system administrator or an IT support executive, and then asks for passwords
  - ***Bribery*** – collecting classified information using bribe
    - A malicious user conducts research on a target employee through social networks looking for specific traits
      - Does the employee at a level in the company have the useful information?
      - Is the employee unsatisfied with the company?
      - Is the employee morally elastic?
      - Does the employee have exploitable weakness, such as financial difficulty or addiction to gambling, alcohol or drugs?

Social Engineering (cont.)

- Social engineering techniques
  - ***Deception*** – tricking a victim to take an action or a sequence of actions that reveals sensitive information
    - Example: A malicious user joined an online chatting room and wrote "Hey guys, if you type in '/myhistory' + your password, you can see all the chatting history of yours". (In fact, '/myhistory' is an arbitrary string the malicious user made up.) A victim believed the malicious user and typed in "/myhistory" and his password into the message window, which revealed the password to the malicious user.
  - ***Conformity*** – convincing a victim that the malicious user and the victim have a lot in common and share the same values.
    - The malicious user becomes the victim's good friend to obtain useful information.

Social Engineering *(cont.)*

- Countering social engineering ***as a software developer***
  - Be aware of social engineering techniques. Update your knowledge for such new techniques.
  - Protect users' personal information (user-centric data and privacy management)
  - Establish and enforce an information security policy that thoroughly addresses social engineering attacks.

Social Engineering *(cont.)*

- ***Educate users*** about social engineering
  - Do not provide any information to unknown people
  - Do not disclose any confidential information to anyone over the social networks
  - Do not type passwords or other confidential information in front of unknown people
  - Do not submit information to any insecure Web site.
  - Do not use the same username and password for all accounts.
  - Verify the credentials of persons asking for confidential information
  - Recognize that authentic system administrators do not need your password to access your files.

References

- A. Basta and W. Halton, *Computer Security and Penetration Testing*, Thomson, 2008, Chapter 2
- R. Krutz and A. Fry, *The CSSLP Prep Guide: Mastering the Certified Secure Software Lifecycle Professional*, Wiley, 2010, Chapter 5