Social Networking Security

Adam C. Champion and Dong Xuan
CSE 4471: Information Security
Outline

• Overview of Social Networking
  – On-line Social Networking
  – Mobile Social Networking
• Threats and Attacks
• Defense Measures
Online Social Networking (OSN)

• Online Web services enabling people to connect with each other, share information
  – Common friends, interests, personal info, …
  – Post photos, videos, etc. for others to see
  – Communicate via email, instant message, etc.

• Major OSN services: Facebook, Twitter, MySpace, LinkedIn, etc.
“Giving people the power to share and make the world more open and connected.”
OSN Popularity

• Over 900 million Facebook users worldwide [6]
  – Over 150 million in U.S. [5]
  – Over 450 million access via mobile [6]
  – 300 million pictures uploaded to Facebook daily [6]
• Over 140 million Twitter users; over 340 million Tweets sent daily [7]
• Over 175 million LinkedIn members in over 200 countries [8]
Benefits of OSN Communication

• Vast majority of college students use OSNs
  – Organizations want to market products, services, etc. to this demographic
  – OSNs can help them reach these potential buyers

• OSNs provide communal forum for expression (self, group, mass), collaboration, etc.
  – Connect with old friends, find new friends and connect
  – Play games with friends, e.g., Candy Crush
  – Commerce in “virtual items”

• But using OSNs poses security issues for orgs as well as individuals
Mobile Social Networking

• E-SmallTalker

• E-Shadow
Application Scenario: Conference
Background: Small Talk

• People come into contact opportunistically
• Face-to-face interaction
  – Crucial to people's social networking
  – Immediate non-verbal communication
  – Helps people get to know each other
  – Provides the best opportunity to expand social network
• Small talk is an important social lubricant
  – Difficult to identify significant topics
  – Superficial
Naive Approach: Smartphone-based Small Talk

- Store all user information, including each user’s full contact list
- Users report either their own geo-location or a collection of physically nearby phone IDs to the server using Internet connection or SMS
- Server performs profile matching, determines small talk topics (mutual contact, common interests, etc.)
- Results are pushed to or retrieved by users
However......

- Require costly data services (phone’s internet connection, SMS)
- Require reporting and storing sensitive personal information on third-party servers
- Trusted server may not exist!
- Centralized servers are bottlenecks, single point of failures, targets of attack
E-SmallTalker: A Fully Distributed Approach

- No Internet connection required
- No trusted third party
- No centralized server

- Information stored locally on mobile phones
- Original personal data never leaves a user’s phone
- Communication only happens in physical proximity
E-Shadow

• Enhanced E-SmallTalker
  – Local profiles
  – Mobile phone based local social interaction tools
    • E-Shadow publishing
    • E-Shadow localization
Outline

• Overview of Social Networking
• Threats and Attacks
• Defense Measures
OSN Security Threats/Attacks

- Malware distribution
- Cyber harassment, stalking, etc.
- Information “shelf life” in cyberspace
- Privacy issues:
  - Information about person posted by him/herself, others
  - Information about people collected by OSNs
- Information posted on OSNs impacts unemployment, insurance, etc.
- Organizations’ concerns: brand, laws, regulations
MSN Security Threat/Attacks

• Personal information leakage
  – Particularly dangerous because of physical proximity
• Malware distribution
Outline

• Overview of Social Networking
• Threats and Attacks
• Defense Measures
“Common Sense” Measures (1)

- Use strong, unique passwords
- Provide minimal personal information: avoid entering birthdate, address, etc.
- Review privacy settings, set to “maximum privacy”  
  - “Friends of friends” includes far more people than “friends only”
- Exercise discretion about posted material:  
  - Pictures, videos, etc.
  - Opinions on controversial issues
  - Anything involving coworkers, bosses, classmates, professors
  - Anything related to employer (unless authorized to do so)
- Be wary of third party apps, ads, etc. (P.T. Barnum’s quote)
- Supervise children’s OSN activity
“Common Sense” Measures (2)

• “If it sounds too good to be true, it probably is”
• Use browser security tools for protection:
  – Anti-phishing filters (Chrome, Firefox)
  – Web of Trust (crowdsourced website trust)
  – AdBlock/NoScript/Do-Not-Track Plus
• Personal reputation management:
  – Search for yourself online, look at the results…
  – Google Alerts: emails sent daily to you about results for any search query (free), e.g., your name
• Extreme cases:
  – Cease using OSNs, delete accounts
  – Contact law enforcement re. relentless online harassment
E-SmallTalker: Privacy-Preserved Information Exchange

- Example of Alice’s Bloom filter
- Alice has multiple contacts, such as Bob, Tom, etc.
- Encode contact strings, Firstname.lastname@phone_number, such as “Bob.Johnson@5555555555” and “Tom.Mattix@6141234567”
E-Shadow: Layered Publishing

• Spatial Layering
  – WiFi SSID
    • At least 40–50 meters, 32 bytes
  – Bluetooth Device (BTD) Name
    • 20 meters, 2,000 bytes
  – Bluetooth Service (BTS) Name
    • 10 meters, 1,000 bytes

• Temporal Layering
  – For people lingering together long or repeatedly
  – Erasure code
Final Remarks

- Online social networking systems very popular; mobile social networking systems emerging
- Malware distribution, personal info. leakage: the two most prominent threats and attacks
- Personal countermeasures are most effective
References (1)


References (2)

17. https://twitter.com/BPglobalPR