Privacy Protection for Social Networking APIs

Adrienne Felt and David Evans
University of Virginia

W2SP, May 2008
privacy protection for social networking APIs
Facebook Platform

- Third parties get screen real estate
- User information available to developers
  - Installed users and their friends
- Backend code and databases are on third-party servers
privacy protection for social networking APIs
Architecture

1. profile.php?

2. app content?
   user=12345

3. API calls

4. app content
   FBML

5. Convert to HTML

6. full page
   HTML/JS

privacy protection for social networking APIs
Architecture

1. profile.php?

6. full page HTML/JS

2. app content?

4. app content

5. Convert to HTML

3. API calls

privacy protection for social networking APIs
Architecture

1. profile.php?

2. app content?
   user=12345

3. API calls
   + permissions check

4. app content
   FBML

5. Convert to HTML

6. full page
   HTML/JS

privacy protection for social networking APIs
Architecture

1. profile.php?

2. app content?
   user=12345

3. API calls

4. app content

5. Convert to HTML

6. full page
   HTML/JS

privacy protection for social networking APIs
Architecture

1. profile.php?

6. full page
   HTML/JS

2. app content?
   user=12345

3. API calls

4. app content
   FBML

5. Convert to HTML
Architecture

1. profile.php?

2. app content?
   user=12345

3. API calls

5. Convert to HTML

6. full page
   HTML/JS

privacy protection for social networking APIs
FBML

• No need to make API calls for many cases
• Large subset of HTML
• + extra fancy Facebook tags
  - fb:pronoun, fb:if-is-friends-with-viewer
  fb:board, fb: comments, fb:random
FBML example

"My user ID is: " . $user;
"My name is: <fb:name uid='" . $user . "'/>";
"Choose a friend: <fb:friend-selector idname='friendsel'/>";
privacy protection for social networking APIs
Facebook Policy

Add Movies to your Facebook account?

- Know who I am and access my information
- Put a box in my profile
- Place a link in my left-hand navigation

Granting access to information is required to add applications. If you are not willing to grant access to your information, do not add this application.
Applications need data

- Can harness social graphs & connections
- Tailor applications to user interests
Should they have data?

- Developers can’t always be screened
- Once data is off the server...can’t police it
- Even trusted applications are security weak points
Application Needs

What kind of data?

- None: 100%
- Public: 0%
- Private: 0%

study of 150 most popular apps, fall 07

How is it used?

- N/A: 100%
- Display: 0%
- Use: 0%
Privacy protection

- Only give applications information if they need it
  - Abstract the user with FBML tags
- Minimize how they need it
  - More sophisticated tags
privacy protection for social networking APIs
Privacy Goals

• User IDs can’t be mapped back to user names
  - Application-specific IDs

• User account information is invisible
  - FBML tags keyed by IDs
Application IDs

- User IDs are encrypted with an application key
  - Can’t be used to reverse lookup users
- Returned by tags like the friend-selector
Privacy by proxy

1. profile.php?

2. app content?
   $\text{user}_{\text{enc}}=12345$

3. app content
   FBML
   $<$user="12345"
   field="birthday">

4. Convert to HTML

5. full page
   HTML/JS

November 8, 1986
Permissions Check

1. profile.php?

2. app content?
   user_enc=12345

3. app content
   FBML
   <user="12345"
   field="birthday">

4. Convert to HTML
   check
   page viewer &
   page owner

5. full page
   HTML/JS
   November 8, 1986
• Attacker could iterate through IDs to list public information
• Disallow lookup of strangers
  - Only owner privileges affected
Functionality

breakdown of 150 most popular apps, fall 07

- wall posting: 5%
- messages & gifts: 25%
- viral recruiting: 10%
- top scorers: 15%
Contact List

• Superset of friend list
• New addition: one-way relationships
• Alice messages Bob; Now Bob can “see” Alice.
Privacy by proxy

234
birthdate, 234
politics, 234

8472
birthdate, 8472
politics, 8472

583
birthdate, 583
politics, 583

586
birthdate, 586
politics, 586

privacy protection for social networking APIs
Initiating contact

- 234 birthday, 234 politics, 234
- 8472 birthday, 8472 politics, 8472
- 583 birthday, 583 politics, 583
- 586 birthday, 586 politics, 586
View with contact list

234
birthdate, 234
politics, 234

8472
birthdate, 8472
politics, 8472

111
birthdate, 111
politics, 111

583
birthdate, 583
politics, 583

586
birthdate, 586
politics, 586

835
birthdate, 835
politics, 835

privacy protection for social networking APIs
Impact of contact lists

- Message-passing works fine now
- Top scorers still affected
  - Not crucial to application
  - In-game profiles, nicknames
OpenSocial

- Google provides a “standardized” API
- Still in beta, differs slightly between sites
- Applications written in XML and then transformed
Conclusion

• Most applications don’t need access to full user information

• Many can be satisfied with anonymous users and server-side transformations

• Applicable to both Facebook and OpenSocial
Questions?

Adrienne Felt
felt@cs.virginia.edu