Privacy Leakage in Mobile Online Social Networks

Balachander Krishnamurthy, AT&T Labs – Research
Craig E. Wills, Worcester Polytechnic Institute

Workshop on Online Social Networks

Boston, MA USA

June 2010

Introduction

Previously studied the leakage of personally identifiable information via Online Social Networks (OSNs) to third-party aggregators.

Trend towards use of mobile devices to access OSNs (Facebook reports 25% of users access OSN via a mobile device every month).

Also development of *new* OSNs—mobile OSNs (mOSNs)—that primarily cater to mobile users. Examples include Brightkite, Foursquare, Gowalla, Loopt, Urbanspoon, Whrrl.

Mobile access to Web sites designed specifically for mobile devices and through the development of "apps" that are specific to a site and to a mobile platform.

New Privacy Concerns

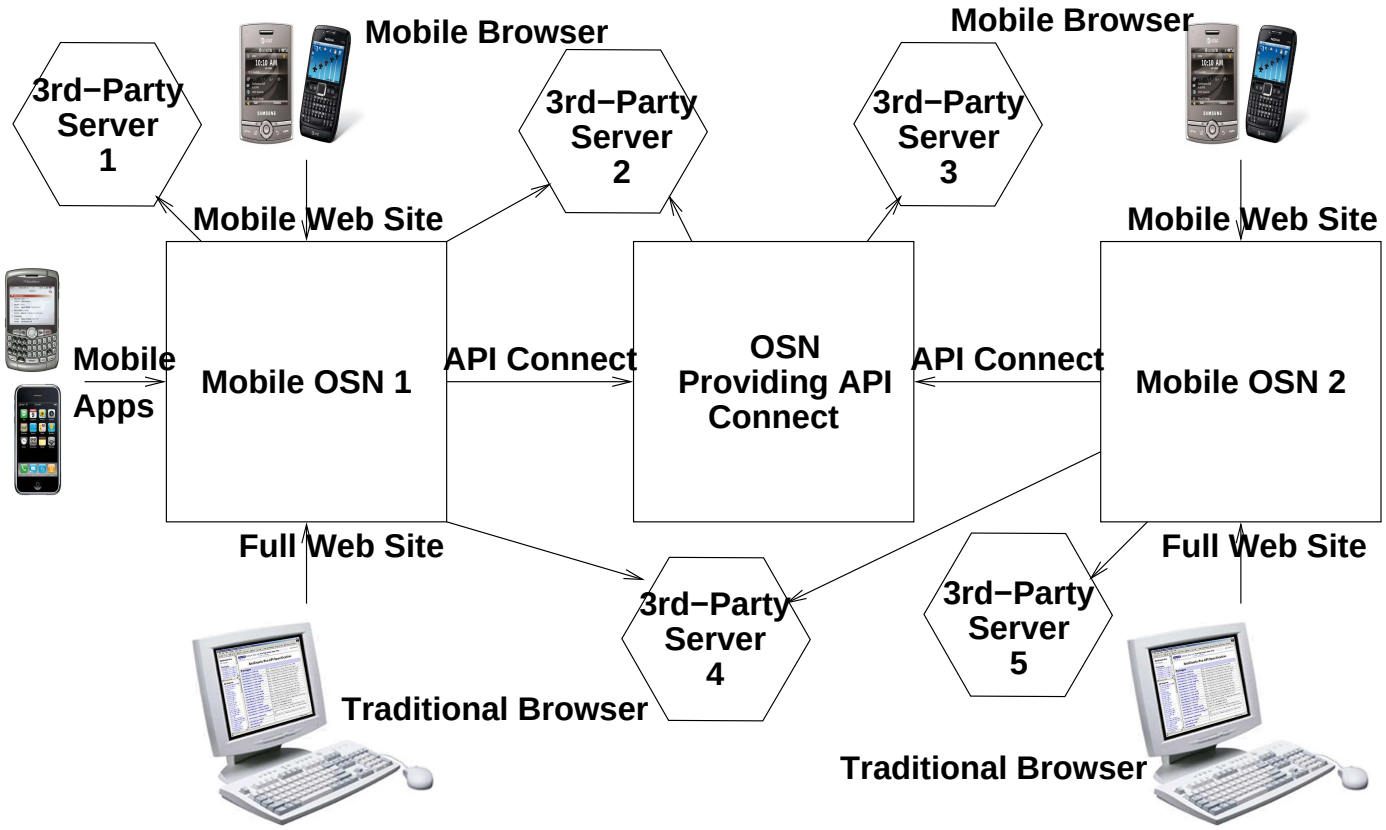
Mobile devices potentially introduce new privacy concerns for mOSNs. These include:

- user presence and geographic location
- information shared with a mOSN connected to a traditional OSN is also shared with that OSN
- unique device identifiers

Examine the degree to which leakage of private information is occurring via mOSNs.

Related work by Chen&Rahman'08 on analyzing privacy designs of social networking apps focusing on location.

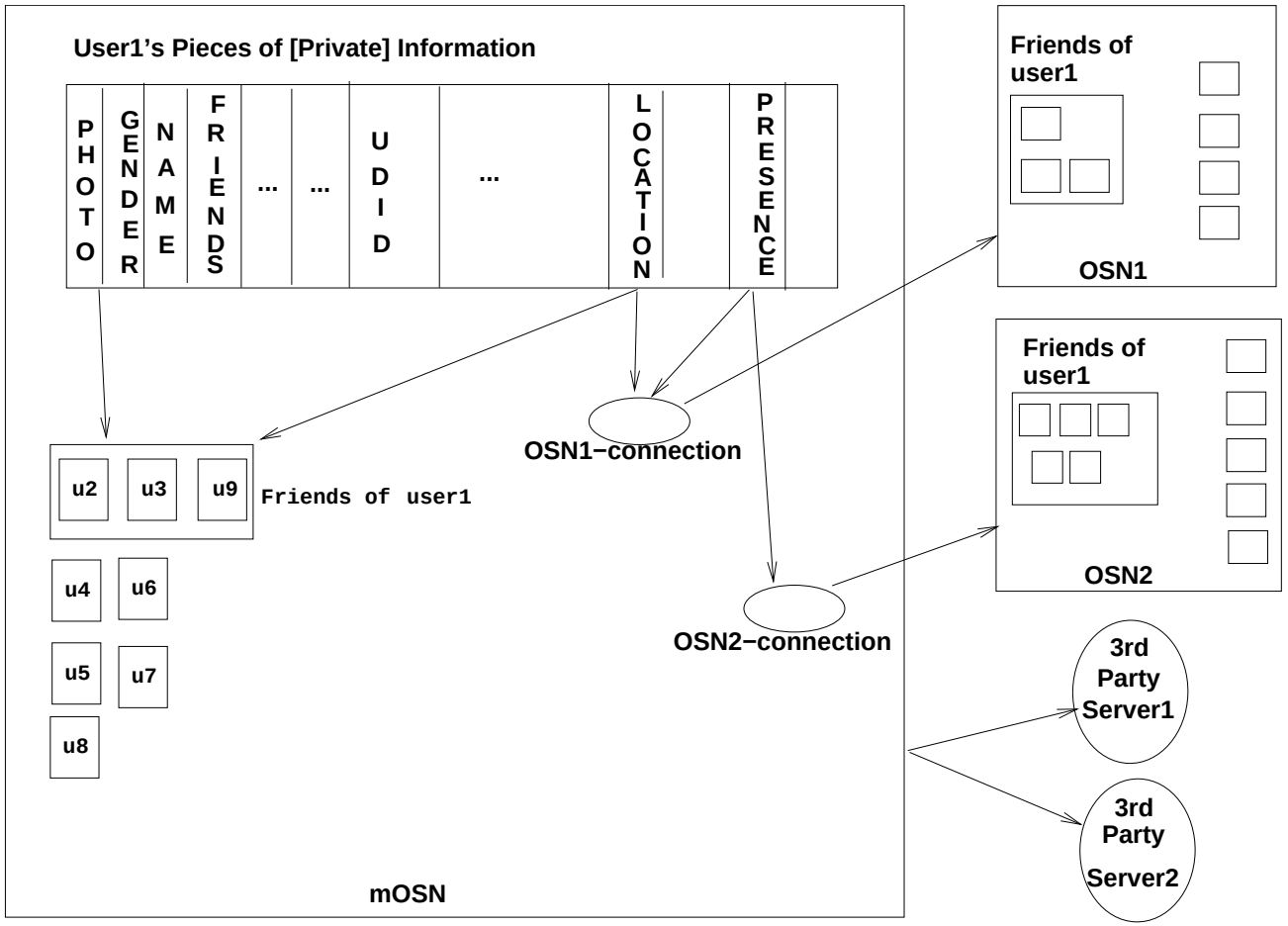
Interfaces and Interconnections for mOSNs



Interfaces include full Web site, mobile Web site and mobile app.

Connections with OSNs and third-parties.

Potential Privacy Leakage Vectors in mOSNs



Privacy Issues

Many mOSNs have a "check-in" mechanism—both establishes a user's *presence* on the mOSN and the user's current *location*.

Mobile devices typically have a unique device identifier, which is often used as verification for installing approved apps on a user's mobile device.

If this unique identifier is leaked to a third-party via an application and can be associated with a user's identity, this becomes a privacy problem.

Linkage between mOSNs and traditional OSNs.

Mobile OSNs for Study

Focused on mOSNs requiring accounts by users, supporting concept of friends, and providing at least one interface with content tailored for mobile devices.

Used popularity metrics as a secondary criterion to establish a study set of 20 mOSNs.

Re-examined seven mOSNs with roots as a traditional OSN:
Bebo, Facebook, Hi5, Linkedin, Livejournal, MySpace and Twitter.

Added two special-purpose social networks: Flickr, Yelp.

Added 11 mOSNs not in existence prior to the widespread use of mobile devices: Brightkite, Buzzd, Dopplr, Foursquare, Gowalla, Gypsii, Loopt, Radar, Urbanspoon, Wattpad and Whrrl.

Mobile Device Applications

Not a specific criterion for inclusion in our study, but found the following count of applications (out of 20) for each device:

- Apple iPhone—19
- Blackberry—10
- Google Android—6
- Palm—6
- Microsoft Windows Phone—3

Research Issues

1. Availability of user information within mOSNs
2. Location and presence
3. Interconnectedness of mOSNs
4. Leakage to third-parties
5. Leakage of new PII to third-parties

Methodology

Examined each available interface for 19 of the mOSNs (all but Hi5) using the Apple iPhone application as the app interface.

Used a Web proxy to capture HTTP traffic for full and mobile Web sites.

Almost all applications also used HTTP for communication, which was capturable with proxy. Network sniffer revealed no leakage for non-HTTP traffic.

Recorded multiple sessions for each mOSN interface while performing actions appropriate for the given interface.

Availability of PII Pieces to Users in 13 mOSNs

Piece of PII	Level of Availability			
	Always Available	Available by default	Unavailable by default	Always Unavailable
Personal Photo	10	3	0	0
Home Location	3	4	1	1
Gender	2	3	1	3
Name	5	5	1	2
Friends	6	6	0	1
Activities	3	7	1	0
Photo Set	0	3	0	0
Age/Birth Year	1	3	0	2

We note that these 13 mOSNs request and make available less information about each user in comparison to OSNs previously studied.

Each mOSN allows the sharing of information to be controlled by a user via the full Web site interface of the mOSN.

Only a minority of these mOSNs provide any privacy settings via the mobile and mobile application interfaces.

Location and Presence

Seven traditional OSNs: 5 provide means to post public comments (presence), but only one allow a user to establish a current location.

Of the 13 others:

Information	Level of Availability			
	Always Available	Available by default	Unavailable by default	Always Unavailable
Check-In Location	3	3	2	5
Comments	4	7	1	1

Location available by default to all mOSN users for roughly half of the mOSNs with comments available by default for most mOSNs.

Interconnectedness of mOSNs

Number of mOSNs with Connections to Twitter, Facebook and Flickr (out of 12 excluding seven traditional plus Flickr):

- Twitter—10
- Facebook—8
- Flickr—2

Actions in mOSNs passed through to these OSNs, but not privacy controls.

A user's location may now be posted to all on Facebook or Twitter.

Example Leakage of OSN Identifier

```
GET /e0?rt=1&amp;...
Host: p.admob.com
Referer: http://buzzd.com/m/buzz/.../id/OSN-ID
Cookie: uuid=ef07qb76f47b19173389f27a9ae1d391
```

Via Referer Field of Buzzd Mobile Web Site

Example of Direct PII Leakage

```
GET /ad_source.php?d[gender]=m...
Host: r.admob.com
X-Admob-Isu: IPHONE-UDID
Cookie: uuid=ef07qb76f47b19173389f27a9ae1d391
```

Direct PII Leakage to a Third-Party Via Request-URI of Radar App (since deceased).

Example Leakage of User Location

```
POST http://beacon.pinchmedia.com/
Host: beacon.pinchmedia.com
User-Agent: buzzd/2.2.0 CFNetwork/459
     Darwin/10.0.0d3

beacons="did":"IPHONE-UDID",..
     ”lat” : ”20.00”, ”lon” : ”-70.00”
```

Location Leakage to a Third-Party Via POST from Buzzd App

Observe that the location is shared with a map service by the application interface of eight mOSNs, the mobile Web site of four mOSNs and the full Web site of one mOSN.

Counts of Known Third-Party Privacy Leakage via 20 mOSNs

What is Leaked?	Leakage Interface		
	Mobile	App	Full
OSN Identifier	6	2	18
Piece of PII	1	2	5
Location	0	2	0

Type of Leakage: Explicit Vs. Implicit

Do *not* know intention when leakage occurs, but can classify leakage into two types:

1. *Explicit* if leak via Request-URI or POST. Difficult to prevent unless done so on a per-server basis.
2. *Implicit* if leak via Referer or Cookie header. Possible for user to prevent.

Explicit leakage for 9 of 26 instances of OSN identifier leakage.

All leakage instances of PII pieces and location are explicit leakage.

Example Leakage of Unique Device Identifier to Third-Parties

```
GET /?i=xxxxxxxx-xxxx-...&u=IPHONE-UDID
Host: ads.mobclix.com
User-Agent: Wattpad/1.6.1 CFNetwork/459
     Darwin/10.0.0d3
```

Observed such explicit leakage for six mOSNs.

Some type of private information is leaked to a third-party via all 20 of the mOSNS in our study.

Summary

Leakage problems found earlier in traditional OSNs continue to be a problem with new mOSNs.

New leakages found—location, device identifiers.

Multi-dimensional privacy protection problem for the user: including duration of privacy settings, transitive closure of information arising from connections with traditional OSNs, what information is shared with different OSNs and third parties.

Needs continued monitoring as sites evolve.

Also need to extend app study to a broader set of devices.