Controlling How Mobile Apps Expose Privacy Sensitive Data

Peter Hornyack1, Seungyeop Han1, Jaeyeon Jung2, Stuart Schechter3, and David Wetherall12

1CSE, University of Washington 2Intel Labs Seattle 3Microsoft Research
{pjh, syhan}@cs.washington.edu, jaeyeon.jung@intel.com, stus@microsoft.com, djw@cs.washington.edu

Motivation

- Little knowledge about how apps use users' personal data
- Have access to location, phone IDs, address book, camera, network ...
- All-or-nothing install-time permissions neglect context
- When/Where user is, Destination, App's status

Goals

- Understand how real apps use privacy sensitive data
  - By using TaintDroid logs over various Android apps.
- Build smart, flexible system to control exposure of the data
  - Extend TaintDroid to enforce policies

- TaintDroid monitors information flow of personal data and alerts users when the data leaves the phone

Example Application

- Bump: a popular data sharing app.
  - Sends out IMEI number periodically (every second)
  - Sends out location and accelerometer data when data sharing happens

Current & Future work

- Policy database
  - Stores exposure policy based on context and user’s preferences
  - When application attempts to send out personal data, database is queried and policy is enforced
- Finding better policies
  - Fine-grained policies per app and per context
  - Efficient ways to get users’ feedback and create useful exposure policies
  - Reducing private information In sent data

System

Example Policies: Certified servers Advertising servers Unknown servers

<table>
<thead>
<tr>
<th></th>
<th>Certified servers</th>
<th>Advertising servers</th>
<th>Unknown servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictive</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Whitelist</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Blacklist</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

Query policy database

runtime tracking of mobile apps
41° 53' N 87° 38' W
41° 53' N 87° 38' W
41° 53' N 87° 38' W
3D view
The Duke of Palm
app server
app server
ad server
monitoring sensor accesses
Network interface
Controlling data exposure
41° 53' N 87° 38' W