Enhancing Security and Privacy on Android

Jeff Foster

Associate Professor and
Associate Chair for Graduate Education
Department of Computer Science and UMIACS

Joint work with Jinseong Jeon, Kristopher K. Micinski, Jeffrey A. Vaughan, Ari Fogel, Nikhilesh Reddy, Philip Phelps, Todd Millstein
Android Popularity

- Android — most popular smartphone platform
  - 70.1% of the market in 4Q12
  - 850K Android apps on Google Play (Apr. 2013)
  - 40 billion apps downloaded (Apr. 2013)

- Apps can be distributed by anyone
  - Easy to install app from any site
Permissions on Android

- Permissions associated with resources and OS features
  - Internet, GPS, telephony, ...

- Permissions granted at install time
  - once granted, apps can use such permissions any way they want
Finer-grained Permissions

- **Goal:** Introduce finer-grained permissions
  - E.g., Gasbuddy has full access to Internet
  - But only needs access to gasbuddy.com

- **Benefits of finer-grained permissions**
  - Help *app developers*
    - improve apps’ robustness against security exploits
    - attest to apps’ proper usage of permissions
  - Help *users*
    - understand how apps use permissions

- Also, aim to do this without changing platform
Example Finer-grained Permissions

- Internet ➔ *InternetURL*(d)
  - InternetURL(gasbuddy_com)

- GPS ➔ *TruncatedLoc*(d)
  - Resolution up to distance d

- Phone state ➔ *PhoneState*(p)
  - PhoneState(UniqueID)
Our Tool Chain

- **RefineDroid** infers how permissions are used in the app
- **Dr. Android** retrofits the app with fine-grained permissions
- **Mr. Hide** enforces fine-grained permissions at runtime
RefineDroid

- infers how permissions are used
  - string analysis to search URL-like strings
  - constant propagation to determine key parameters to privileged APIs
  - e.g. for system settings:

    ```java
    Uri uri = Uri.parse("my_ringtone.mp3");
    RingtoneManager.setActualDefaultRingtoneUri(
        this, RingtoneManager.TYPE_ALARM, uri);
    String path = uri.toString();
    Settings.System.putString(
        getContentResolver(),
        Settings.System.RINGTONE, path);
    ```

Dr. Android

- Dalvik Rewriter for Android
  - injects hidelib.dex
  - modifies the app’s bytecode to use Mr. Hide
  - removes Android perms. and adds Mr. Hide perms.
Mr. Hide

- the Hide interface to the droid environment
  - services
    - interact with a client app and resources
  - client-side library
    - a drop-in replacement for sensitive APIs
## Toolchain Results

<table>
<thead>
<tr>
<th>Feature</th>
<th>Amazon</th>
<th>Angry Birds</th>
<th>Angry Birds Rio</th>
<th>ASTRO</th>
<th>Baby Monitor</th>
<th>GasBuddy</th>
<th>Horoscope</th>
<th>Shazam</th>
<th>Google Sky Map</th>
<th>Task Killer</th>
<th>Brightest Flashlight</th>
<th>Ultimate Flashlight</th>
<th>Qrdroid</th>
<th>Radar Now!</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>INTERNET</code></td>
<td>● ● ● ●</td>
<td>○ ● ● ● ○ ●</td>
<td>○ ○ ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ●</td>
</tr>
<tr>
<td><code>READ_CONTACTS</code></td>
<td>● ● ● ●</td>
<td>○ ● ● ● ○ ●</td>
<td>○ ○ ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ●</td>
</tr>
<tr>
<td><code>ACCESS_*_LOCATION</code></td>
<td>● ● ● ●</td>
<td>○ ● ● ● ○ ●</td>
<td>○ ○ ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ●</td>
</tr>
<tr>
<td><code>READ_PHONE_STATE</code></td>
<td>● ● ● ●</td>
<td>○ ● ● ● ○ ●</td>
<td>○ ○ ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ●</td>
</tr>
<tr>
<td><code>WRITE_SETTINGS</code></td>
<td>● ● ● ●</td>
<td>○ ● ● ● ○ ●</td>
<td>○ ○ ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ● ● ● ● ● ● ● ●</td>
<td>● ● ●</td>
<td>● ● ●</td>
</tr>
<tr>
<td>InternetURL(·)</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>ContactCol(·)</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>LocationBlock</td>
<td>✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>ReadPhoneState(UniqueId)</td>
<td>✔ ✔</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>WriteSettings(Ringtone)</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
</tr>
</tbody>
</table>

- Applied to 14 apps
- that exercise our fine-grained permissions
- 31 out of 35 uses of perms. are replaced correctly
- not always appropriate: e.g. `sftp` feature of ASTRO

build-in Android perm.  
●: can be replaced  
○: cannot be replaced  
✖: over-privileged  

fine-grained perm.  
✔: needed, and being used
A Study of Location-Based Apps

- Studied effect of $d$ in $TruncatedLoc(d)$ permissions
- Research literature: several location-privacy enhancing techniques
  - Including location truncation
- But not much evaluation of resulting utility
Location Truncation

- Use Dr. Android and Mr. Hide to intercept location requests
- Snap true latitude/longitude to user-specified grid

Pros:
- Limits localization attacks
- Simple to implement and understand

Cons:
- May defeat with sequences of observations
Study Design

- 6 apps that produce *lists* of nearby objects

- Ran those apps on a variety of locations:
  - 6 population centers (New York, NY to Decatur, TX)
  - 10 points per population center, chosen at random
  - 10 truncation amounts
    - 0, 0.1, 0.2, 0.5, 1, 2, 5, 10, 20, 50km

- Compared output lists before and after truncation
  - Edit distance
  - Set intersection size
  - Additional distance to first item
Example Changed Output

Before truncation

<table>
<thead>
<tr>
<th>Restaurant Finder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading my location...</td>
</tr>
<tr>
<td><strong>China Garden</strong></td>
</tr>
<tr>
<td>(973) 338-9099 0.31 Km</td>
</tr>
<tr>
<td>1060 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>Boonsong Thai Cuisine</strong></td>
</tr>
<tr>
<td>(973) 338-0507 0.34 Km</td>
</tr>
<tr>
<td>1040 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>John Michaels Estate Jewelry</strong></td>
</tr>
<tr>
<td>(973) 338-4400 0.34 Km</td>
</tr>
<tr>
<td>1051 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>Stamna Greek Taverna</strong></td>
</tr>
<tr>
<td>(973) 338-5151 0.35 Km</td>
</tr>
<tr>
<td>1045 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>Bar Cara</strong></td>
</tr>
<tr>
<td>(973) 893-3681 0.37 Km</td>
</tr>
<tr>
<td>1099 North Broad Street Bloomfield, NJ</td>
</tr>
</tbody>
</table>

After truncation

<table>
<thead>
<tr>
<th>Restaurant Finder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading my location...</td>
</tr>
<tr>
<td><strong>IHOP Restaurant</strong></td>
</tr>
<tr>
<td>(973) 893-0151 0.26 Km</td>
</tr>
<tr>
<td>1129 Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>Bar Cara</strong></td>
</tr>
<tr>
<td>(973) 893-3681 0.29 Km</td>
</tr>
<tr>
<td>1099 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>Friendly's Restaurant</strong></td>
</tr>
<tr>
<td>(973) 338-8669 0.44 Km</td>
</tr>
<tr>
<td>1243 Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>China Garden</strong></td>
</tr>
<tr>
<td>(973) 338-9099 0.44 Km</td>
</tr>
<tr>
<td>1060 North Broad Street Bloomfield, NJ</td>
</tr>
<tr>
<td><strong>John Michaels Estate Jewelry</strong></td>
</tr>
<tr>
<td>(973) 338-4400 0.47 Km</td>
</tr>
<tr>
<td>1051 North Broad Street Bloomfield, NJ</td>
</tr>
</tbody>
</table>
Example Additional Distance

[Graph showing additional distance against location truncation for different cities: New York, Dallas, Baltimore, Newhaven, Redmond, Decatur. The graph illustrates the relationship between additional distance and location truncation across various cities.]
Study Results

- Effect of location truncation depends on object density
- Edit distance not a useful metric
  - No good intuitive meaning
- Additional distance is a very forgiving metric
- Many apps/locs can be truncate between 5-20km without significantly degrading utility
Conclusion

- Added fine-grained Permissions to Android
  - RefineDroid, a static analyzer to infer...
  - Mr. Hide, clean interfaces to enforce...
  - Dr. Android, a bytecode rewriter to retrofit...

- Location privacy can be enhanced without degrading utility

- Broader uses
  - other security policies
    - inserting mock data, changing policies at run-time, etc.
  - general support for modifying Dalvik bytecode
Further Information

Jeff Foster
3423 A.V. Williams Bldg (inside MC2)
jfoster@cs.umd.edu

http://www.cs.umd.edu/~jfoster
End