An Empirical Study of the Robustness of Inter-component Communication in Android

Amiya K. Maji, Fahad A. Arshad, Saurabh Bagchi
School of Electrical and Computer Engineering

Jan S. Rellermeyer
IBM Research
Austin, TX, USA

June 28th, 2012

Motivation

“Security flaw lets you bypass lock screen”

“Paper clips pose security threat to iPhones”

“Former McAfee CTO Demos Remote Access Exploits on WebKit”
Overview

• What?
  – Robustness evaluation of smartphones

• Why?
  – To understand and improve the system behavior

• How?
  – Use fuzz testing methodology
  – Generate a large number of semi-valid IPC messages and identify misbehaving apps

• Key Result
  – 10% components CRASHED
  – Uncaught NullPointerExceptions are frequent and pose security threat to Android

Outline

• Android Overview
• Testing Tool (JJB)
• Design Recommendations
• Conclusion
Outline

• Android Overview
• Testing Tool (JJB)
• Design Recommendations
• Conclusion

Android Application Components

• Task
  – Read email
  – Respond to multiple people
Android Application Components

Email Application
- Inbox
- Email
- Reply

Contacts Application
- Select Contact
- Add Contact
- Delete Contact

Components
- Activity
- Service
- Broadcast Receiver
- Content Provider

Intents: Android Communication Primitive

Activity
- Intent

Broadcast Receiver
- Intent

Service
- Content Provider
Structure of Intents

Sender

DIAL: 765-337-5452

action
data

category

extra

Receiver

EMPTY for Implicit Intent

Implicit Intent Resolution to Find a Target Receiver

S

Intent

Intent-Filter

R₁

R₂

R₃

Intent Delivery System

DIAL: 765-337-5452

Sender

action
data

category

extra

Receiver

EMPTY for Implicit Intent

Intent Delivery System

DIAL: 765-337-5452

Sender

action
data

category

extra

Receiver

EMPTY for Implicit Intent

Implicit Intent Resolution to Find a Target Receiver

S

Intent

Intent-Filter

R₁

R₂

R₃

Intent Delivery System
Study Objectives

- Test how robust is Intent handling in Android components
- Discover vulnerabilities through random and crafted Intents
- Recommendations for hardening of Android IPC

Outline

- Android Overview
- Testing Tool (JJB)
- Recommendation
- Conclusion
JarJarBinks (JJB): Robustness Testing Tool

Experimental Configurations

- Tested Android Built-in Apps
  - Android 2.2: Droid [May 2010]
  - Android 4.0: Emulator [Oct 2011]
- Tested Top-5 Android Marketplace Apps (3 Dec, 2011)
  - Facebook
  - Pandora Radio
  - Voxer Walkie Talkie
  - Angry Birds
  - Skype
Intent Generation for Fault Injection Campaign

- Mutated intent-fields
  - Action
  - Data
  - Component
  - Extras
- Target intents by Type
  - Explicit intents
  - Implicit intents

Explicit Intent Generation

- Query Package Manager
  - List Packages
  - Send to Targets
- Four Fault Injection Campaigns (FICs)
  - FIC A: Semi-valid Action AND Data
  - FIC B: Blank Action OR Data
  - FIC C: Random Action OR Data
  - FIC D: Random Extras

\[
\text{Intent \{act=ACTION\_EDIT, data=http://www.google.com \ cmp=com.android.someComponent}\}}
\]

\{ Programming mistakes \}
\{ Active Attacker \}

- FIC A: Semi-valid Action AND Data
FICs: Explicit Intent Generation

- FIC B: Blank Action OR Data

  Intent { data=http://www.google.com cmp=com.android.someComponent}

- FIC C: Random Action OR Data

  Intent {act=ACTION_EDIT data=a1b2c3d4 cmp=com.android.someComponent}

- FIC D: Random Extras

  Intent {act=ACTION_DIAL Data=tel:123-456-7890 cmp=com.android.someComponent has Extras}

Explicit Intents: Crashes on Android 2.2 and 4.0

<table>
<thead>
<tr>
<th>Droid (Android 2.2)</th>
<th>Emulator (Android 4.0)</th>
<th>Marketplace Apps Droid (Android 2.2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activities</td>
<td>Services</td>
<td>Broadcast Receivers</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>297</td>
<td>42</td>
<td>59</td>
</tr>
<tr>
<td># crashed</td>
<td>%</td>
<td># crashed</td>
</tr>
<tr>
<td>Semi-valid</td>
<td>10</td>
<td>10.1</td>
</tr>
<tr>
<td>Blank</td>
<td>21</td>
<td>7.1</td>
</tr>
<tr>
<td>Random</td>
<td>18</td>
<td>6.1</td>
</tr>
<tr>
<td>With Extra</td>
<td>13</td>
<td>4.4</td>
</tr>
</tbody>
</table>

- Lesser crashes in Android 4.0
  - Marketplace apps are more robust
  - Activities crash more often
- Crashes by component type
Explicit Intents: Crashes by Exception Type

- Significant NPE
- Transient Environment Dependent Errors
- App-developer Responsible

System Crash from User-level Application

- No extra permissions at install-time
- 3 Activities crashed Android-Runtime

```
Intent {act=ACTION_X cmp= android/.ActivityX}
```
Implicit Intent Generation

- Valid Intent: match exact intent-filter

- Semi-valid Intent

Implicit Intents: Crashes

<table>
<thead>
<tr>
<th>Exception Type</th>
<th>#Crashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NullPointerException</td>
<td>32</td>
</tr>
<tr>
<td>IOException</td>
<td>22</td>
</tr>
<tr>
<td>RuntimeException</td>
<td>13</td>
</tr>
<tr>
<td>ArrayIndexOutOfBoundsException</td>
<td>6</td>
</tr>
<tr>
<td>android.content.res.Resources$NotFoundException</td>
<td>4</td>
</tr>
<tr>
<td>ClassCastException</td>
<td>3</td>
</tr>
<tr>
<td>TimeoutException</td>
<td>1</td>
</tr>
<tr>
<td>com.sprint.internal.SystemPropertiesException</td>
<td>1</td>
</tr>
<tr>
<td>IllegalArgumentException</td>
<td>1</td>
</tr>
</tbody>
</table>

- Insufficient input-validation
Outline

• Android Overview
• Testing Tool (JJB)
• Design Recommendations
• Conclusion

Recommendation 1: Subtyping

• No explicit contract between sender and receiver
  – Intent Sub-typing

    ```java
    Class CallIntent extends Intent{
    String action="ACTION_DIAL";
    telUri data;
    /*
    getters/setters for fields etc.
    */
    ComponentName cmp;
    }
    ```

• Type checking
  – Static (Java Annotations)
  – Dynamic
Recommendation 2: Domain Specific Language

- Full input-validation
  - Version checks
- Internal DSLs
  - Limited to host language expressiveness
- External DSLs
  - Free-standing

Conclusions

- Robustness testing on Android’s IPC
- Lessons
  - Prevalent Faulty Exception Handling Code (NPE)
  - Android 2.2 Runtime can be crashed by crafted intents
  - Android 4.0 has become robust
- Recommendation for more expressive Intents
  - Sub-typing/ Java annotation
  - DSLs
Thank you

QUESTIONS?

Related Work

• Fuzz Testing [Miller et al, 90,95,00,07]
  – Desktop PCs
• ComDroid [Chin et al, MobiSys 2011]
  – Static analysis tool
• Others
  – Permission assignment [Enck et al, SEC 2011]
  – Application certification [Enck et al, CCS 2009]