

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. Rellermeier
IBM Research
Austin, TX, USA

PURDUE
UNIVERSITY



June 28th, 2012



PURDUE
UNIVERSITY

Motivation



“Security flaw lets you bypass lock screen”

“Paper clips pose security threat to iPhones”

“Former McAfee CTO Demos Remote Access Exploits on WebKit”

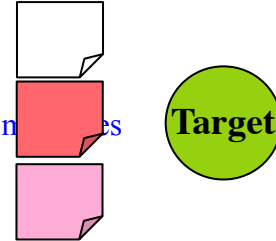


Slide 2

PURDUE
UNIVERSITY

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



Slide 3

PURDUE
UNIVERSITY

Outline

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



Slide 4

PURDUE
UNIVERSITY

Outline

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

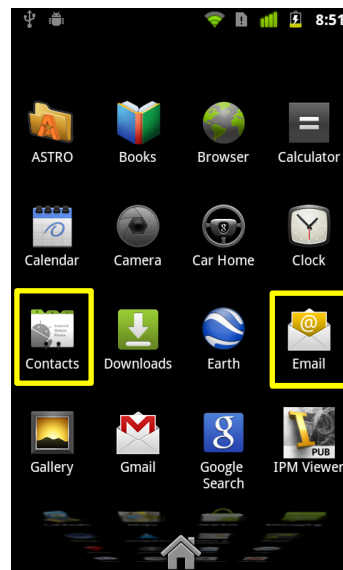


Slide 5



Android Application Components

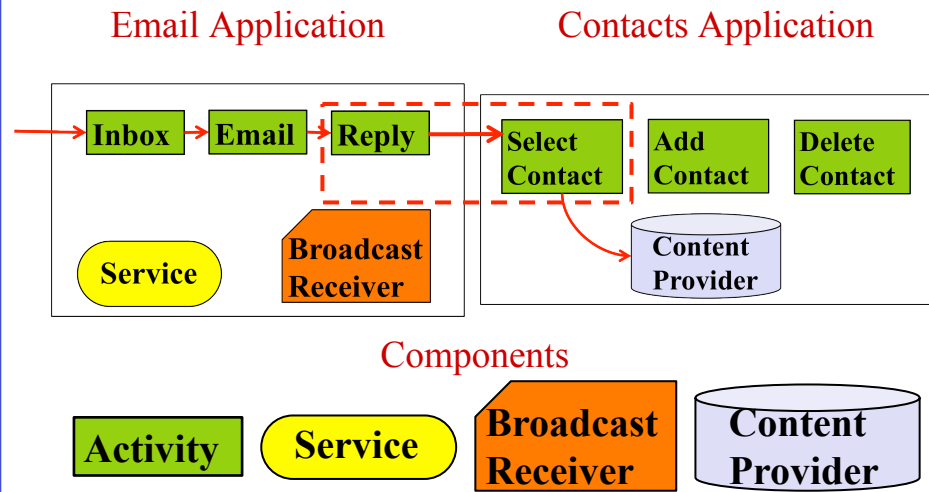
- Task
 - Read email
 - Respond to multiple people



Slide 6



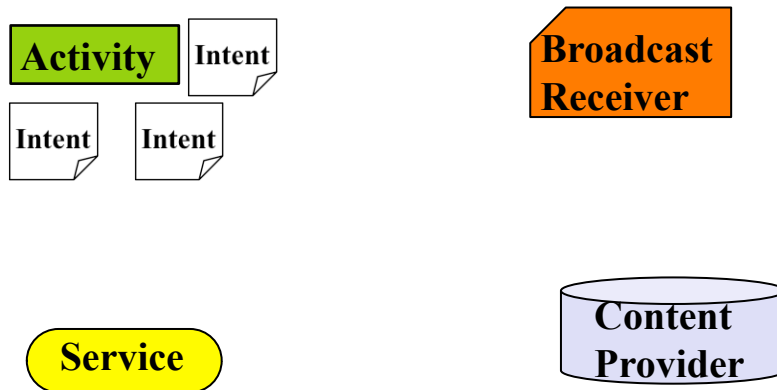
Android Application Components



Slide 7

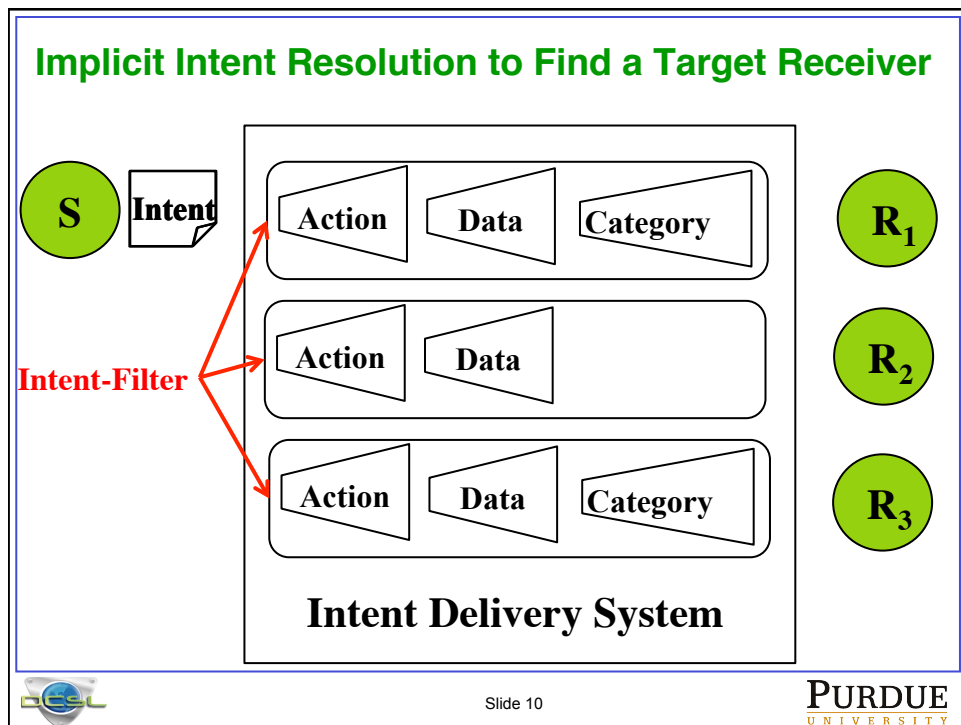
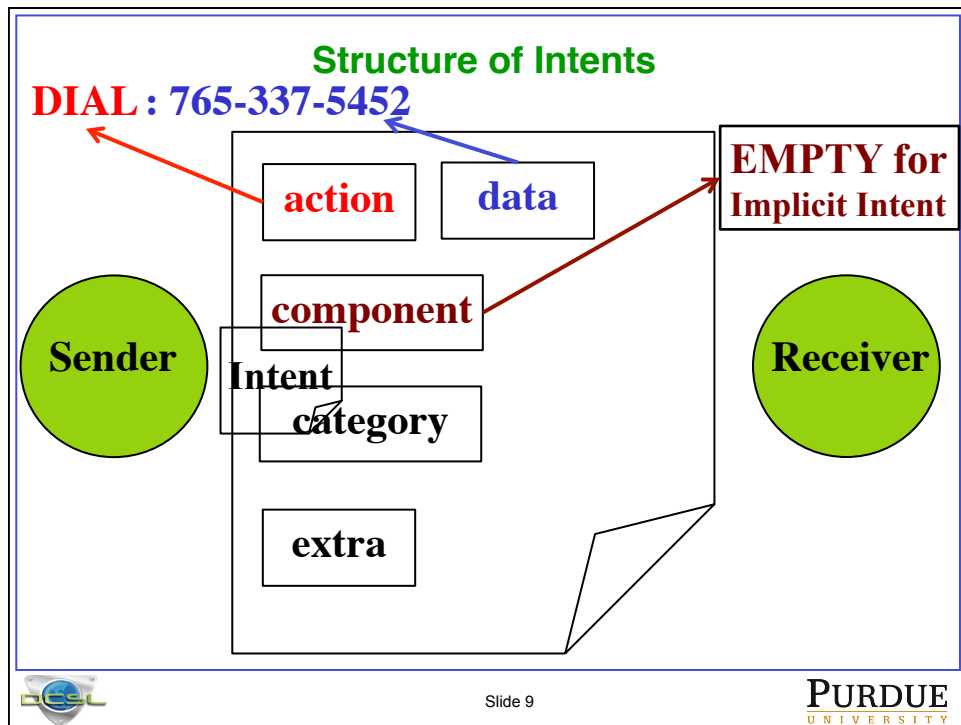
PURDUE
UNIVERSITY

Intents: Android Communication Primitive



Slide 8

PURDUE
UNIVERSITY



Study Objectives

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



Slide 11

PURDUE
UNIVERSITY

Outline

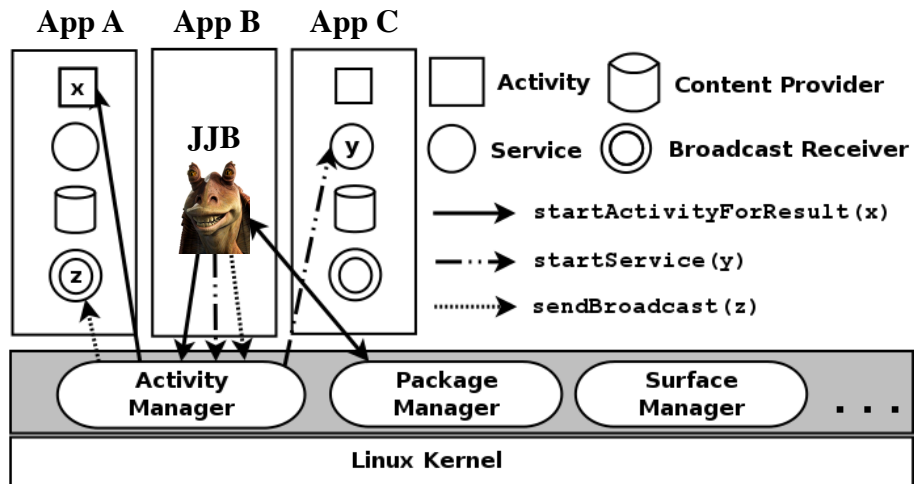
- Android Overview
- Testing Tool (JJB)
- Recommendation
- Conclusion



Slide 12

PURDUE
UNIVERSITY

JarJarBinks(JJB): Robustness Testing Tool



Slide 13

PURDUE
UNIVERSITY

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



Slide 14

PURDUE
UNIVERSITY

Intent Generation for Fault Injection Campaign

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



Slide 15

PURDUE
UNIVERSITY

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

} Programming mistakes

} Active Attacker
- FIC A: Semi-valid Action AND Data

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



Slide 16

PURDUE
UNIVERSITY

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}
```



Slide 17

PURDUE
UNIVERSITY

Explicit Intents: Crashes on Android 2.2 and 4.0

	Droid (Android 2.2)			Emulator (Android 4.0)			Marketplace Apps Droid (Android 2.2)		
	Activities 297	Services 42	Broadcast Receivers 59	Activities 332	Services 54	Broadcast Receivers 69	Activities 103	Services 11	Broadcast Receivers 10
	# crash%	# crash%	# crash%	# crash%	# crash%	# crash%	# crash%	# crash%	# crash%
Semi-valid	30 10.1	1 2.4	2 3.4	29 8.7	3 5.6	2 2.9	4 3.9	0 0.0	0 0
Blank	21 7.1	1 2.4	6 10.2	8 2.4	3 5.6	6 8.7	2 1.9	1 9.1	0 0
Random	18 6.1	1 2.4	4 6.8	9 2.7	3 5.6	2 2.9	2 1.9	0 0.0	0 0
With Extra	13 4.4	1 2.4	1 1.7	7 2.1	3 5.6	0 0.0	3 2.9	0 0.0	0 0

- Lesser crashes in Android 4.0
 - Marketplace apps are more robust
 - Activities crash more often
- Crashes by component type



Slide 18

PURDUE
UNIVERSITY

Explicit Intents: Crashes by Exception Type



• Significant NPE

• Transient Environment Dependent Errors

• App-developer Responsible



Slide 19

PURDUE UNIVERSITY

System Crash from User-level Application

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

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

ActivityX

```
final Bundle extras = getIntent().getExtras();
mAccount = extras.getParcelable(EXTRAS_ACCOUNT);
```

StackTrace

```

I/ActivityManager( 62): Starting activity: Intent { act=ACTION_PACKAGE_DATA_CLEARED cmp=a
android/.accounts.
W/dalvikvm( 62): threadid=7: thread exiting with uncaught exception (group=0x4001d800)
E/AndroidRuntime( 62): *** FATAL EXCEPTION IN SYSTEM PROCESS: android.server.ServerThread
E/AndroidRuntime( 62): Caused by: java.lang.NullPointerException
E/AndroidRuntime( 62): at android.accounts. onCr
eate( java:58)
E/AndroidRuntime( 62): ... more
I/Process ( 62): Sending signal. PID: 62 SIG: 9
I/Zygote ( 33): Exit zygote because system server (62) has terminated
    
```

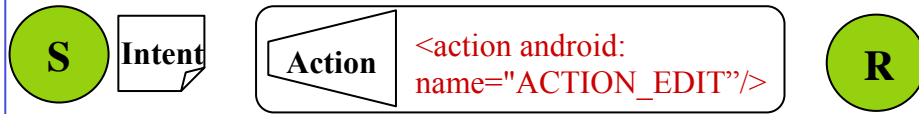


Slide 20

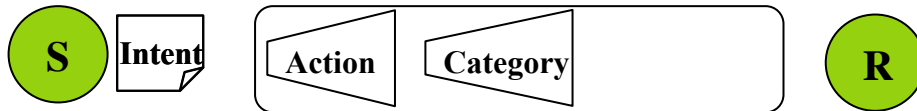
PURDUE UNIVERSITY

Implicit Intent Generation

- Valid Intent: match exact intent-filter



- Semi-valid Intent



Slide 21

PURDUE
UNIVERSITY

Implicit Intents: Crashes

Exception Type	#Crashes
NullPointerException	32
IOException	22
RuntimeException	13
ArrayIndexOutOfBoundsException	6
android.content.res.Resources\$NotFoundException	4
ClassCastException	3
TimeoutException	1
com.sprint.internal.SystemPropertiesException	1
IllegalArgumentException	1

73%

- Insufficient input-validation



Slide 22

PURDUE
UNIVERSITY

Outline

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



Slide 23

PURDUE
UNIVERSITY

Recommendation 1: Subtyping

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

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

- Type checking
 - Static (Java Annotations)
 - Dynamic



Slide 24

PURDUE
UNIVERSITY

Recommendation 2: Domain Specific Language

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



Slide 25

PURDUE
UNIVERSITY

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



Slide 26

PURDUE
UNIVERSITY

Thank you

QUESTIONS ?



Slide 27

PURDUE
UNIVERSITY

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]



Slide 28

PURDUE
UNIVERSITY