

PROGRAMMING HANDHELD SYSTEMS

ADAM PORTER

PERMISSIONS

TODAY'S TOPICS

ANDROID PERMISSIONS

DEFINING & USING APPLICATION PERMISSIONS

COMPONENT PERMISSIONS & PERMISSIONS-
RELATED APIs

PERMISSIONS

ANDROID PROTECTS RESOURCES & DATA WITH PERMISSIONS

USED TO LIMIT ACCESS TO:

USER INFORMATION – E.G, CONTACTS

COST-SENSITIVE API'S – E.G., SMS/MMS

SYSTEM RESOURCES – E.G., CAMERA

PERMISSIONS

PERMISSIONS ARE REPRESENTED AS STRINGS

IN ANDROIDMANIFEST.XML, APPS DECLARE
THE PERMISSIONS

THEY USE THEMSELVES

THEY REQUIRE OF OTHER COMPONENTS

USING PERMISSIONS

APPLICATIONS SPECIFY PERMISSIONS THEY USE
THROUGH A <USES-PERMISSION> TAG

USERS MUST ACCEPT THESE PERMISSIONS
BEFORE AN APPLICATION CAN BE INSTALLED

USING PERMISSIONS

```
<manifest ... >
```

```
...
```

```
<uses-permission android:name=  
    "android.permission.CAMERA"/>
```

```
<uses-permission android:name=  
    "android.permission.INTERNET"/>
```

```
<uses-permission android:name=  
    "android.permission.ACCESS_FINE_LOCATION"/>
```

```
...
```

```
</manifest >
```

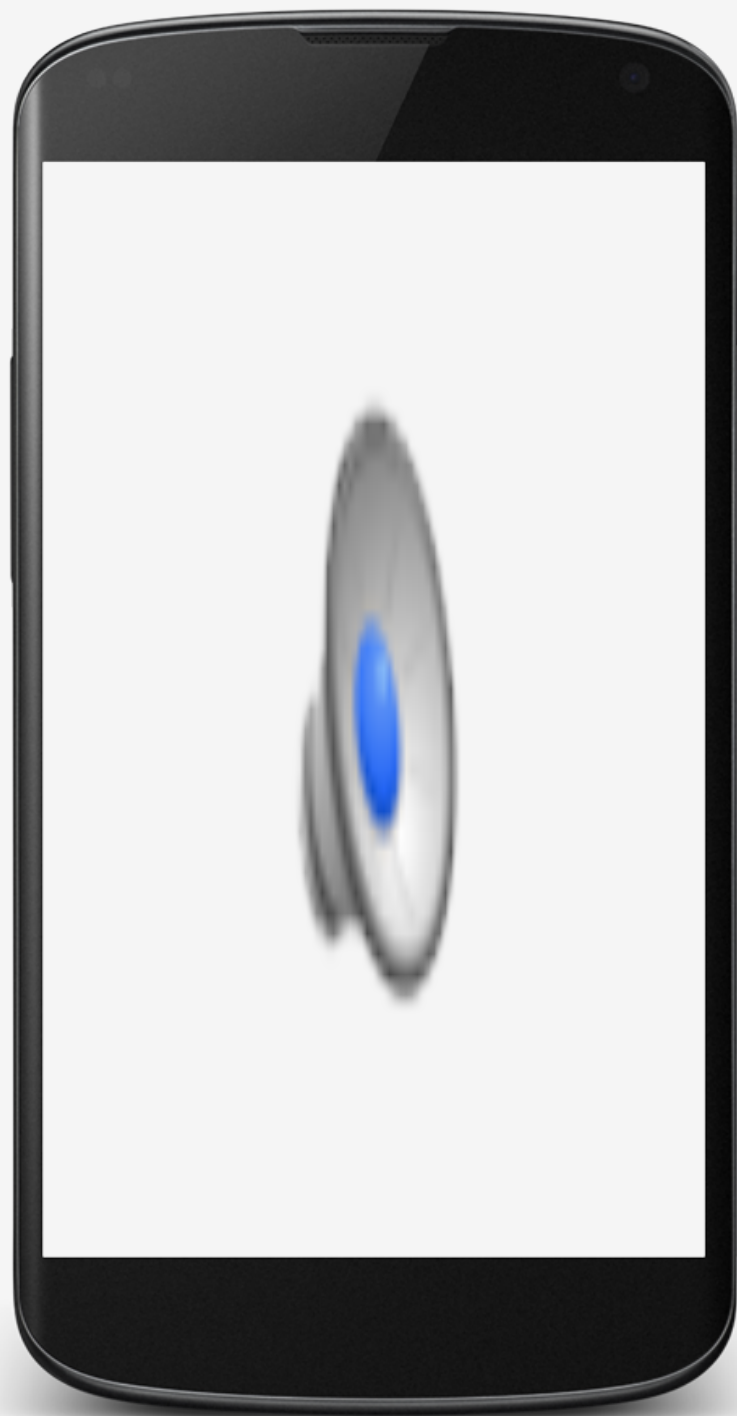
SEE: [HTTP://DEVELOPER.ANDROID.COM/REFERENCE/ANDROID/](http://developer.android.com/reference/android/manifest.permission.html)

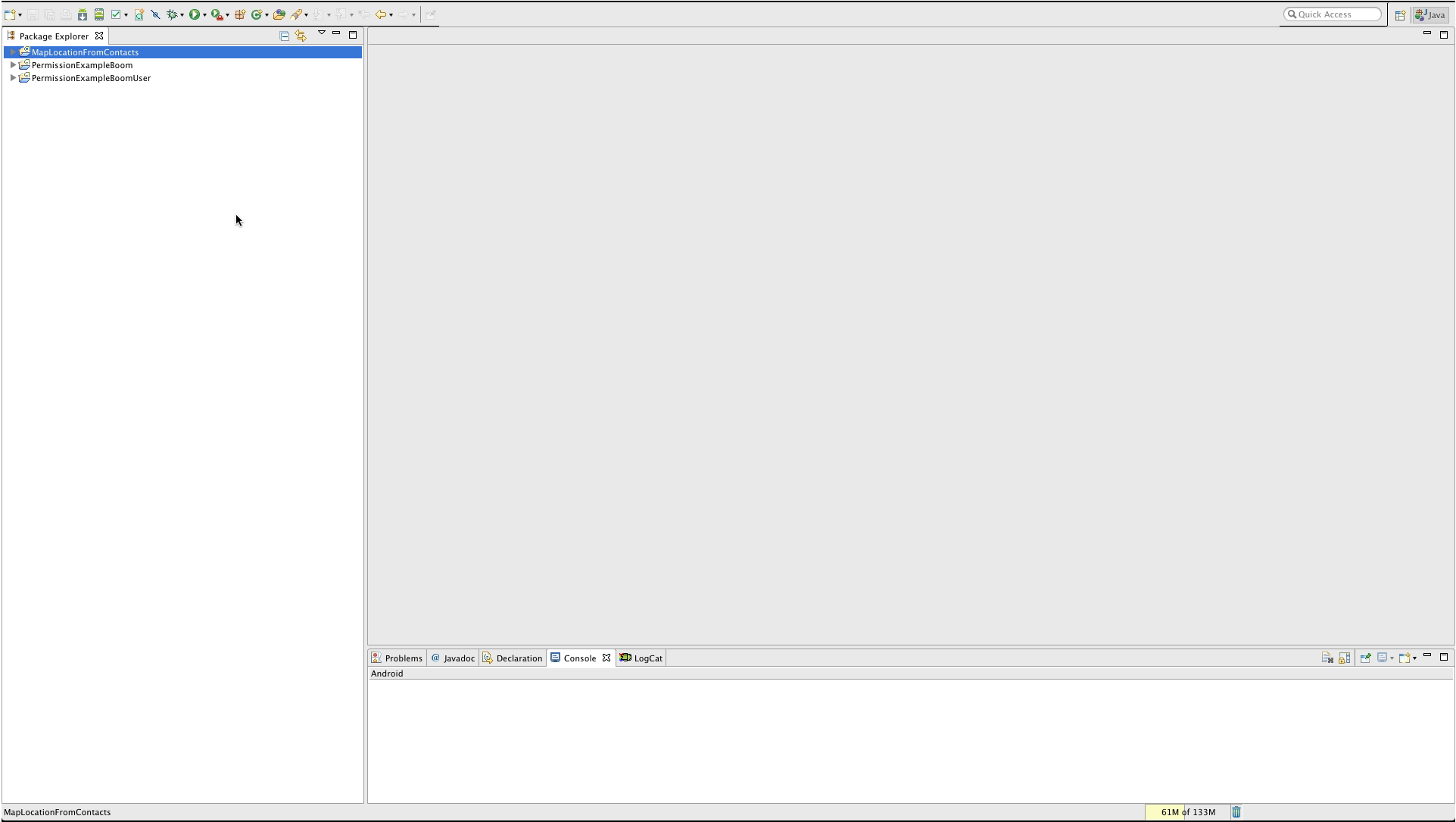
MANIFEST.PERMISSION.HTML

MAPLOCATIONFROMCONTACTS

SELECT A CONTACT FROM CONTACTS
DATABASE

DISPLAY A MAP CENTERED ON SELECTED
CONTACT'S ADDRESS





DEFINING PERMISSIONS

APPS CAN ALSO DEFINE AND ENFORCE THEIR
OWN PERMISSIONS

DEFINING PERMISSIONS

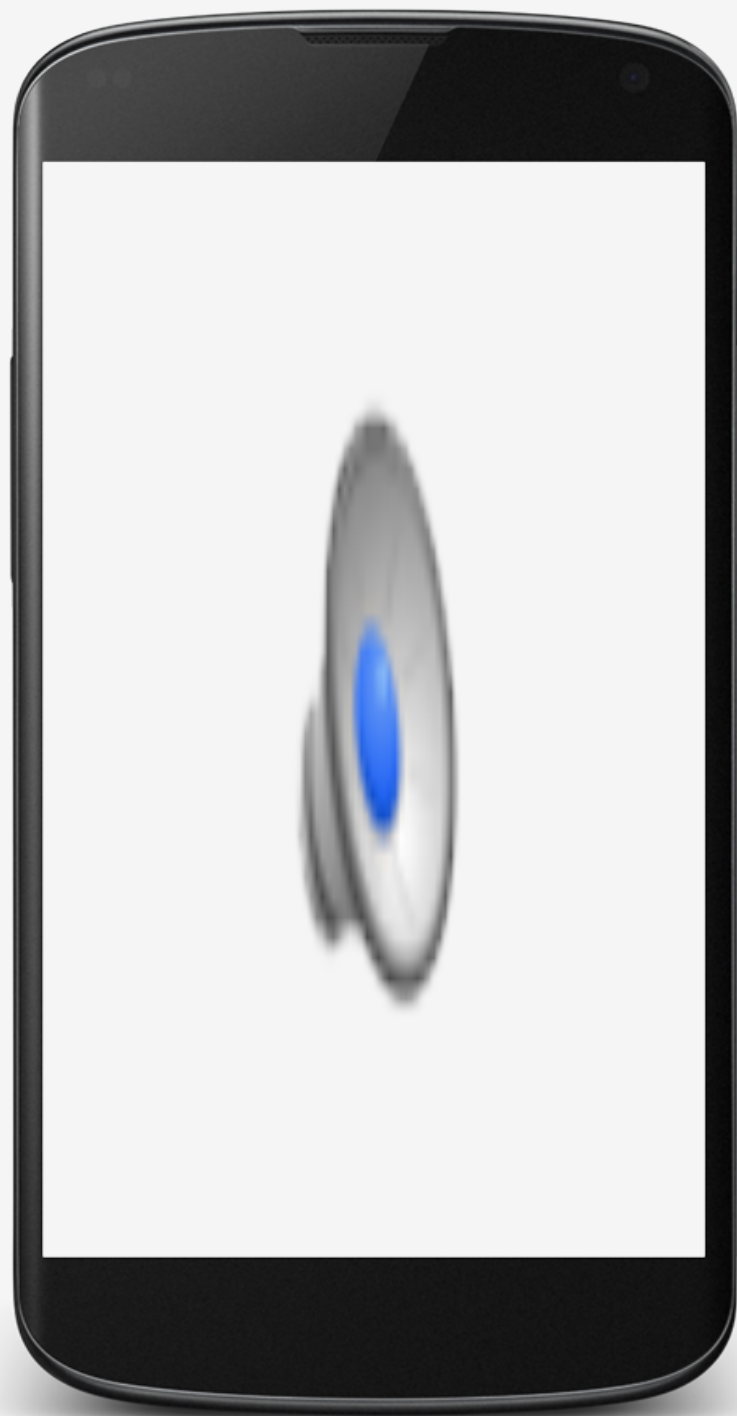
SUPPOSE YOUR APPLICATION PERFORMS A
PRIVILEGED/DANGEROUS OPERATION

YOU MIGHT NOT WANT TO ALLOW JUST ANY
APPLICATION TO INVOKE YOURS

SO YOU CAN DEFINE & ENFORCE YOUR OWN
PERMISSION

PERMISSIONEXAMPLEBOOM

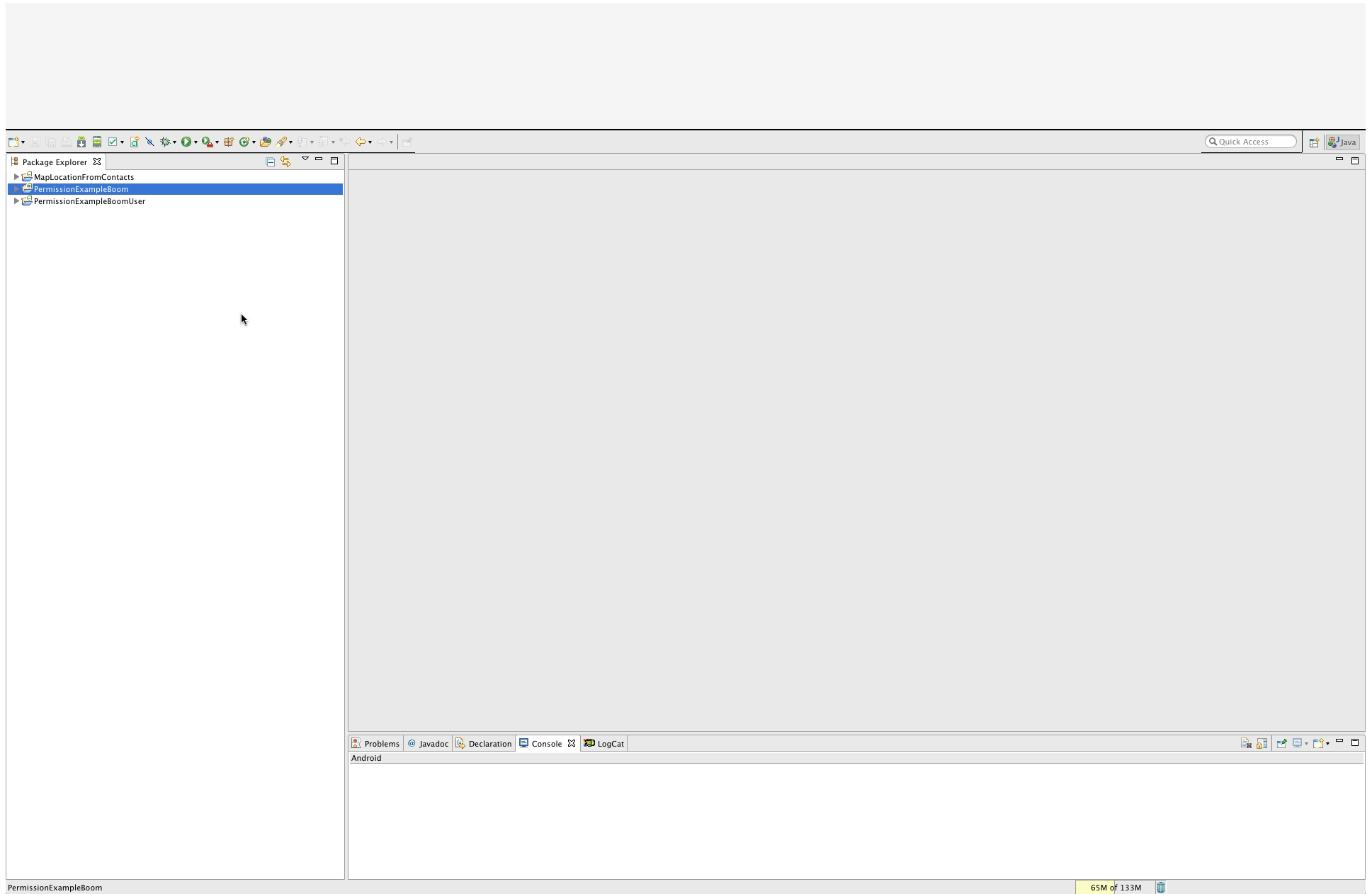
SIMPLE APPLICATION THAT PERFORMS A
(JUST PRETEND) DANGEROUS ACTION



DEFINE & ENFORCING PERMISSIONS

IF YOU DON'T WANT JUST ANYONE TO RUN
PERMISSIONEXAMPLEBOOM

DEFINE & ENFORCE AN APPLICATION-SPECIFIC
PERMISSION



USING THE NEW PERMISSION

APPS THAT WANT TO USE
PERMISSIONEXAMPLEBOOM MUST NOW
ACQUIRE THE CORRECT PERMISSION

Quick Access

Java

Problems

Javadoc

Declaration

Console

LogCat

Saved Filters

+

-

📄

Search for messages. Accepts Java regexes. Prefix with pid., app., tag: to limit scope.

verbose

📄

📄

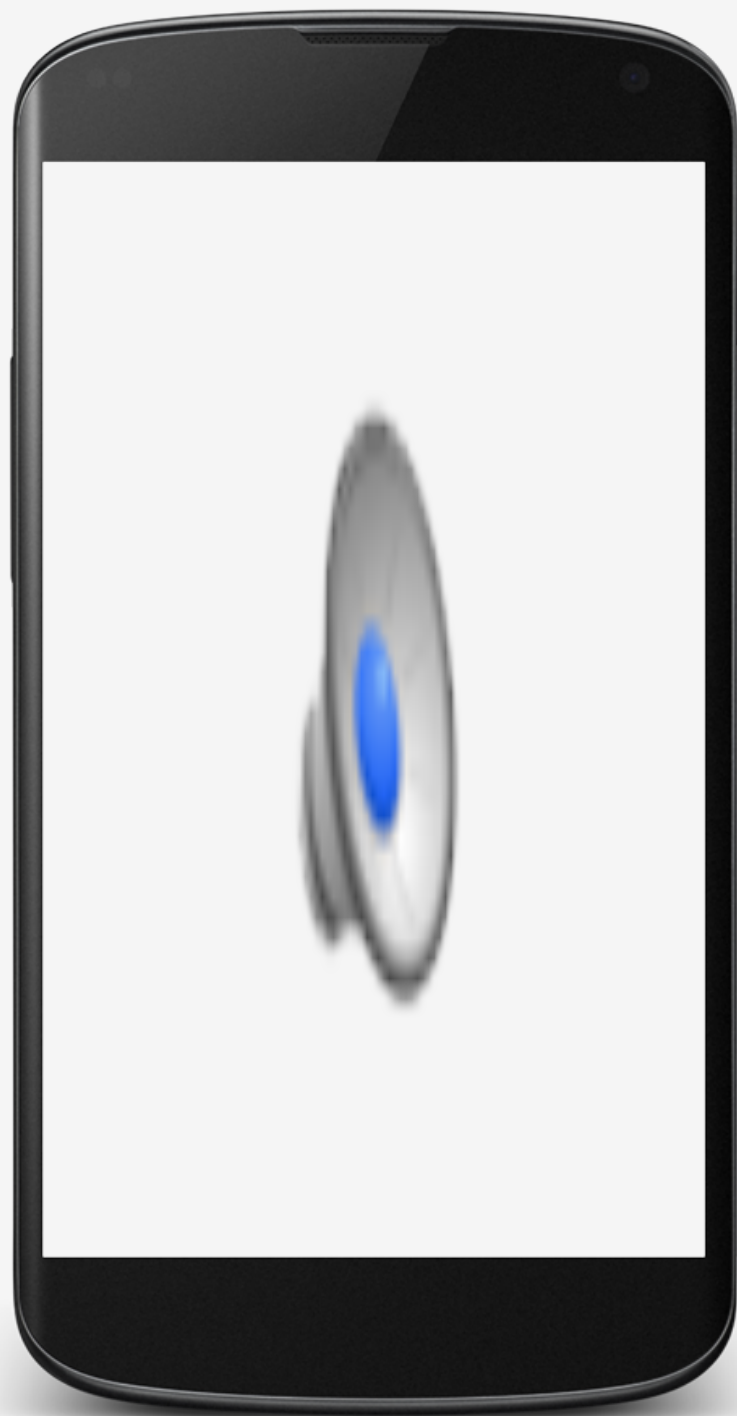
📄

All messages (no filters) (212)

course.examples.permissionexample.boomUser (

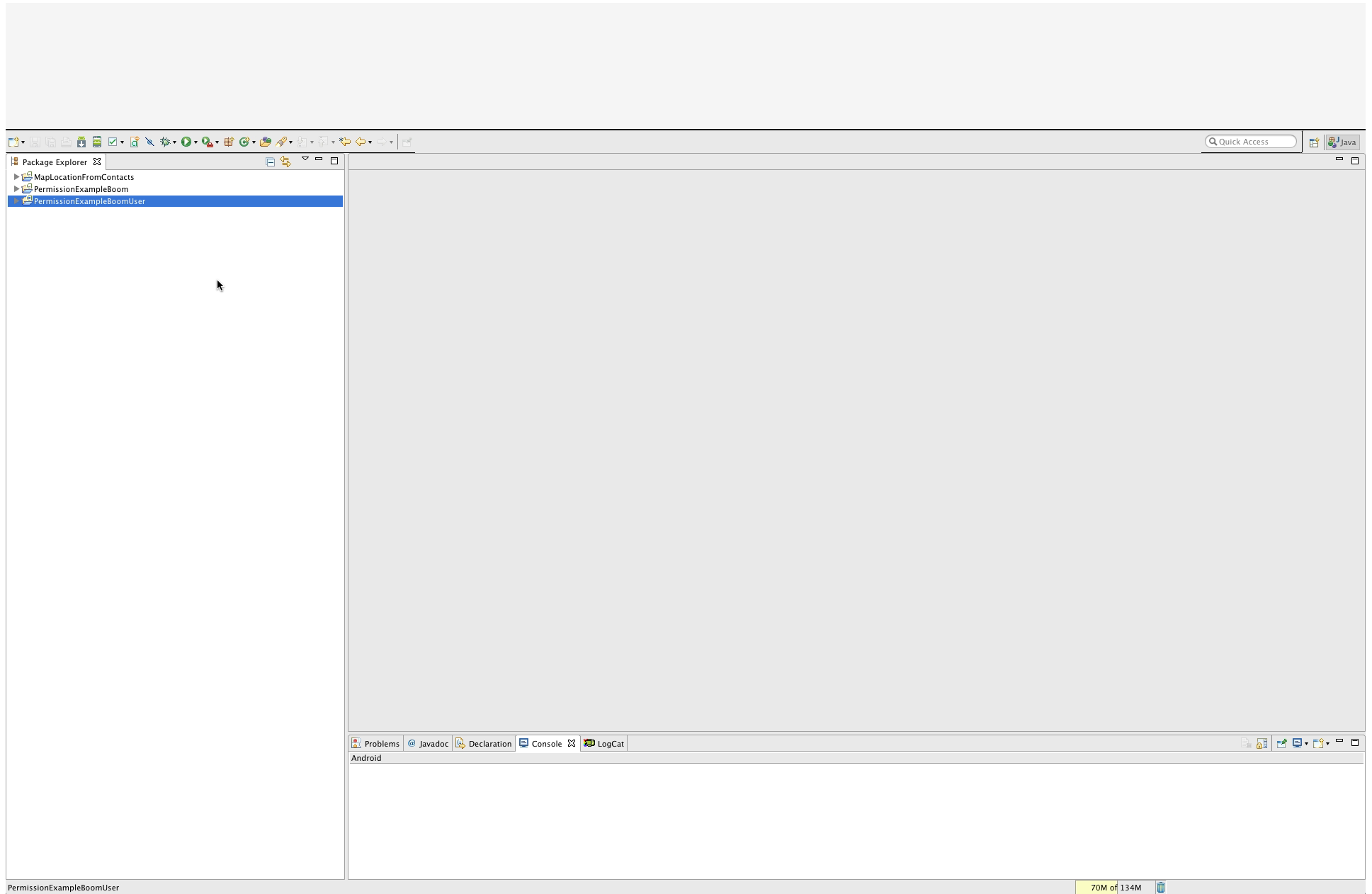
Log Time	PID	TID	Application	Tag	Text
----------	-----	-----	-------------	-----	------

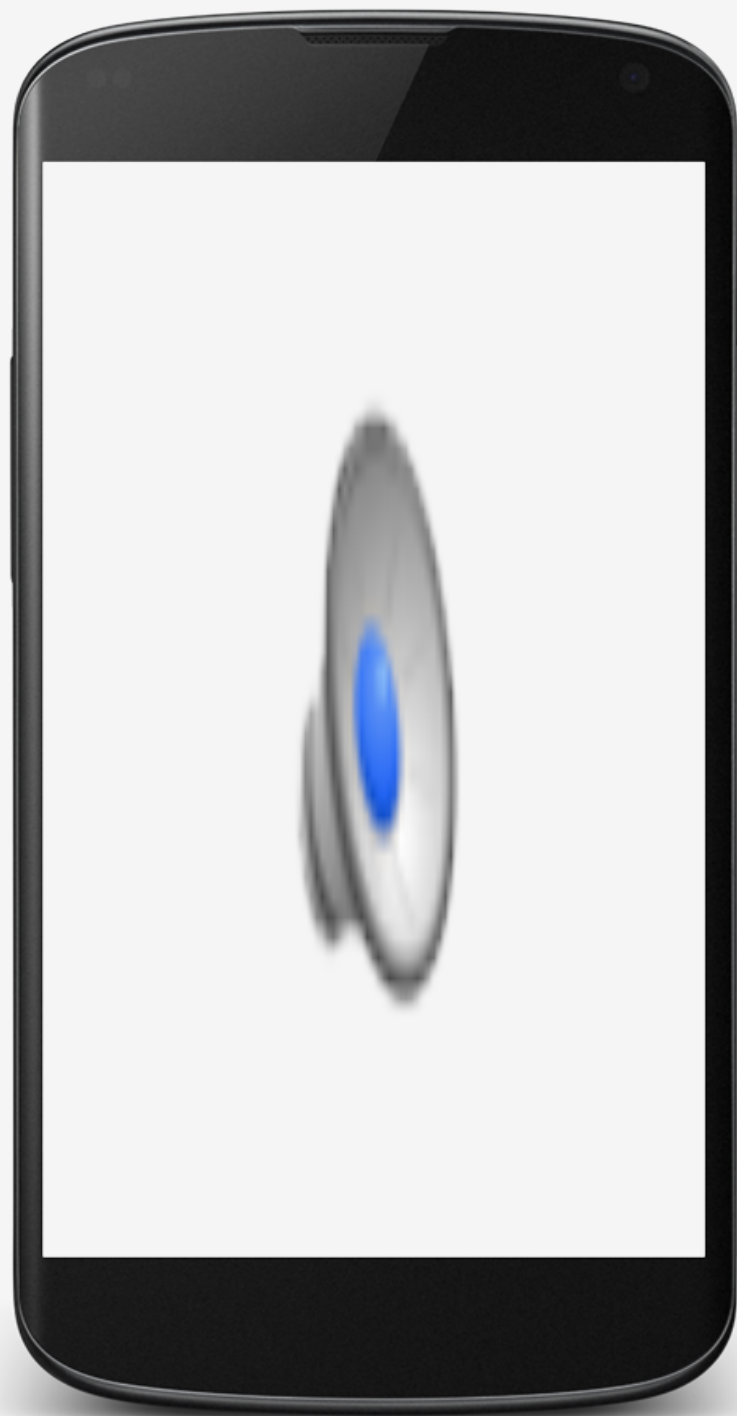
73M of 134M



USES-PERMISSION

AN APPLICATION CAN DECLARE/ACCEPT THE PERMISSIONS OF THE APPLICATIONS IT USES





COMPONENT PERMISSIONS

INDIVIDUAL COMPONENTS CAN SET THEIR OWN PERMISSIONS, RESTRICTING WHICH OTHER COMPONENTS CAN ACCESS THEM

COMPONENT PERMISSIONS TAKE PRECEDENCE OVER APPLICATION-LEVEL PERMISSIONS

ACTIVITY PERMISSIONS

RESTRICTS WHICH COMPONENTS CAN START
THE ASSOCIATED ACTIVITY

CHECKED WITHIN EXECUTION OF

`startActivity()`

`startActivityForResult()`

THROWS `SecurityException` ON PERMISSIONS
FAILURE

SERVICE PERMISSIONS

RESTRICTS WHICH COMPONENTS CAN START
OR BIND TO THE ASSOCIATED SERVICE

CHECKED WITHIN EXECUTION OF

`Context.startService()`

`Context.stopService()`

`Context.bindService()`

THROWS `SecurityException` ON PERMISSIONS
FAILURE

BROADCASTRECEIVER PERMISSIONS

RESTRICTS WHICH COMPONENTS CAN SEND &
RECEIVE BROADCASTS

PERMISSIONS CHECKED IN MULTIPLE PLACES

MORE ON THIS WHEN WE DISCUSS
BROADCASTRECEIVERS

CONTENTPROVIDER PERMISSIONS

RESTRICT WHICH COMPONENTS CAN READ &
WRITE THE DATA IN A CONTENTPROVIDER

MORE ON THIS WHEN WE DISCUSS
CONTENTPROVIDERS

NEXT TIME

THE FRAGMENT CLASS