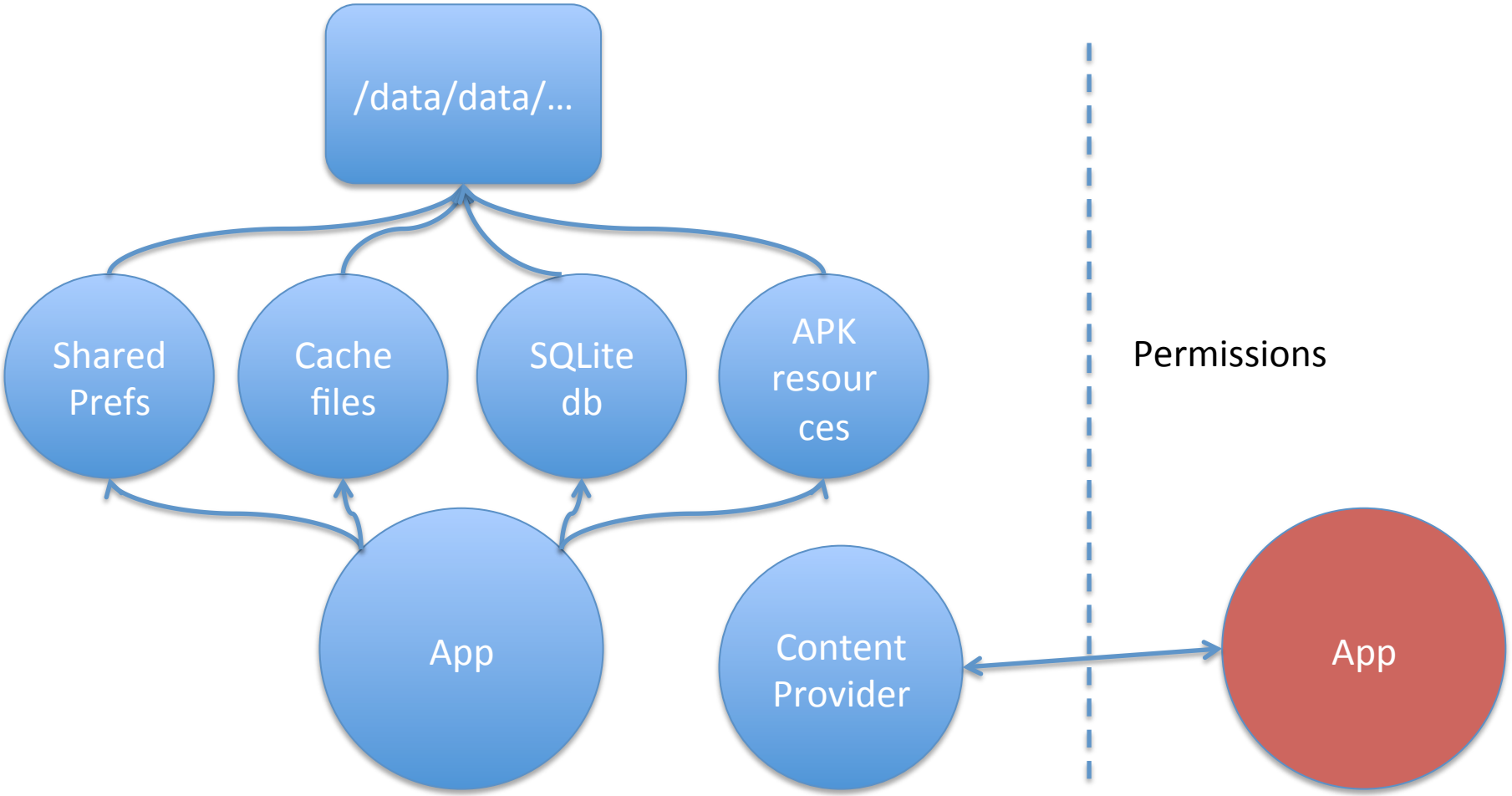
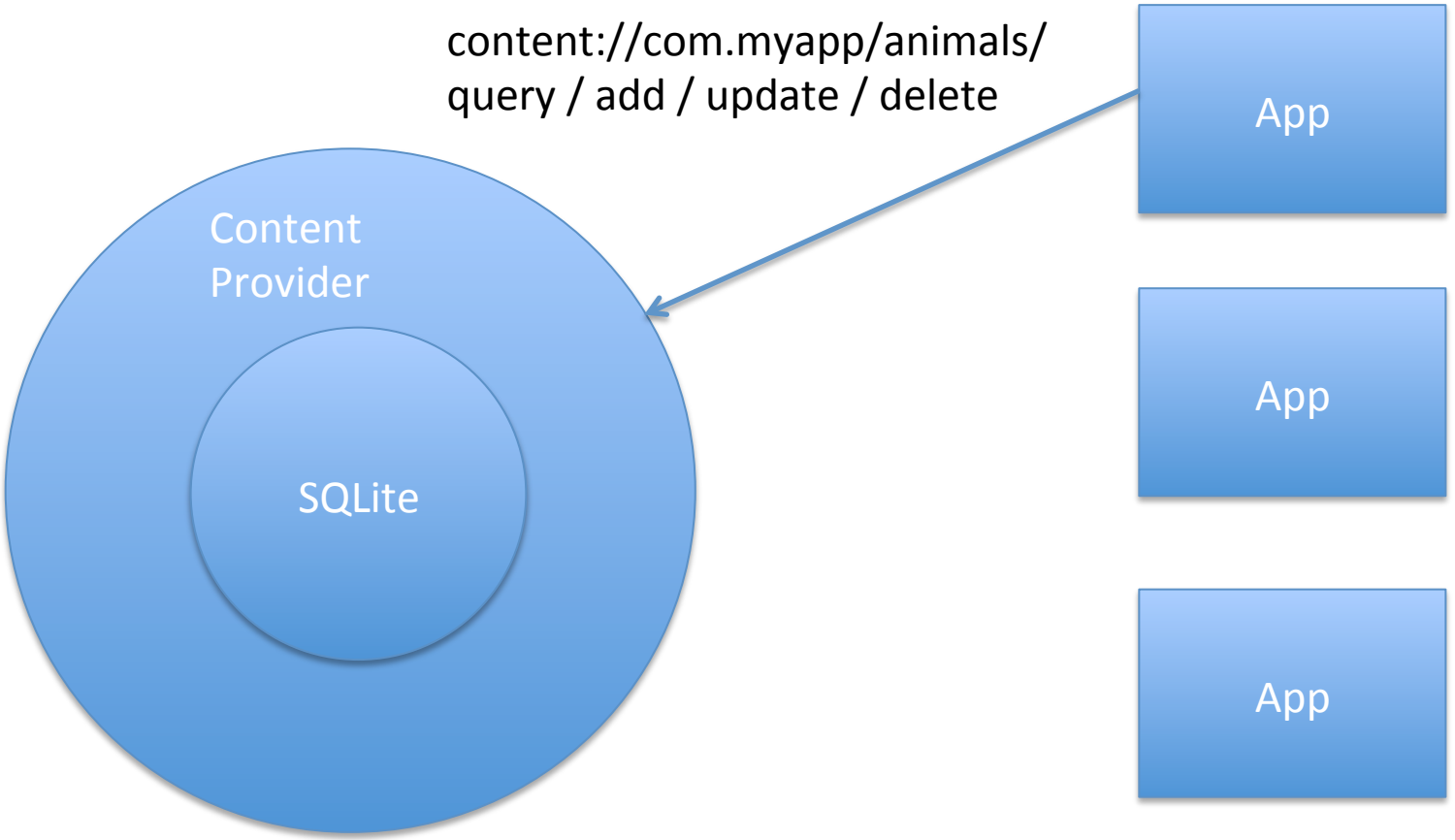
G54MDP
Mobile Device Programming

Lecture 13 –Content Providers and Permissions

Sharing Data – if not



Data Model


content://com.myapp/animals/
query / add / update / delete
App
App
App
Content
Provider
SQLite

Contacts

- To access / modify Contacts, requires a Permission
  - android.permission.READ_CONTACTS
  - android.permission.WRITE_CONTACTS
- Contacts has three components
  - Data
    - Rows (mime-typed) that can hold personal information
  - RawContacts
    - A contact for a given person from a given system
      - Gmail contact, Facebook contact etc
      - Associated with Data entries
  - Contacts
    - Aggregated RawContacts
      - Single view to a person

Modifying a ContentProvider

- Uri insert(Uri url, ContentValues values)
- int update(Uri uri, ContentValues values, String where, String[] selectionArgs)
- Uri
  - The table that we wish to update / insert
- ContentValues
  - Values for the new row
  - Key/value pairs
    - Key is the column name
- where
  - SQL WHERE clause

Creating a Content Provider

- Implement a storage system for the data
  - Structured data / SQLite
    - Values, binary blobs up to 64k
    - Database
  - Large binary blobs
    - Files
  - Photos / media manager
- Implement a ContentProvider
  - Implement required methods
  - query, add, update, insert etc
  - onCreate
  - getType
    - What type of data are we providing?
  - ParcelFileDescripter openFile()
- Tell Android we are a provider
  - Declare in the AndroidManifest

Contract

- Defines metadata pertaining to the provider
- Constant definitions that are exposed to developers via a compiled .jar file
  - Authority
    - Which app is responsible for this data
  - URI
  - Meta-data types
  - Column names
    - Abstraction of database architecture

URI Matching

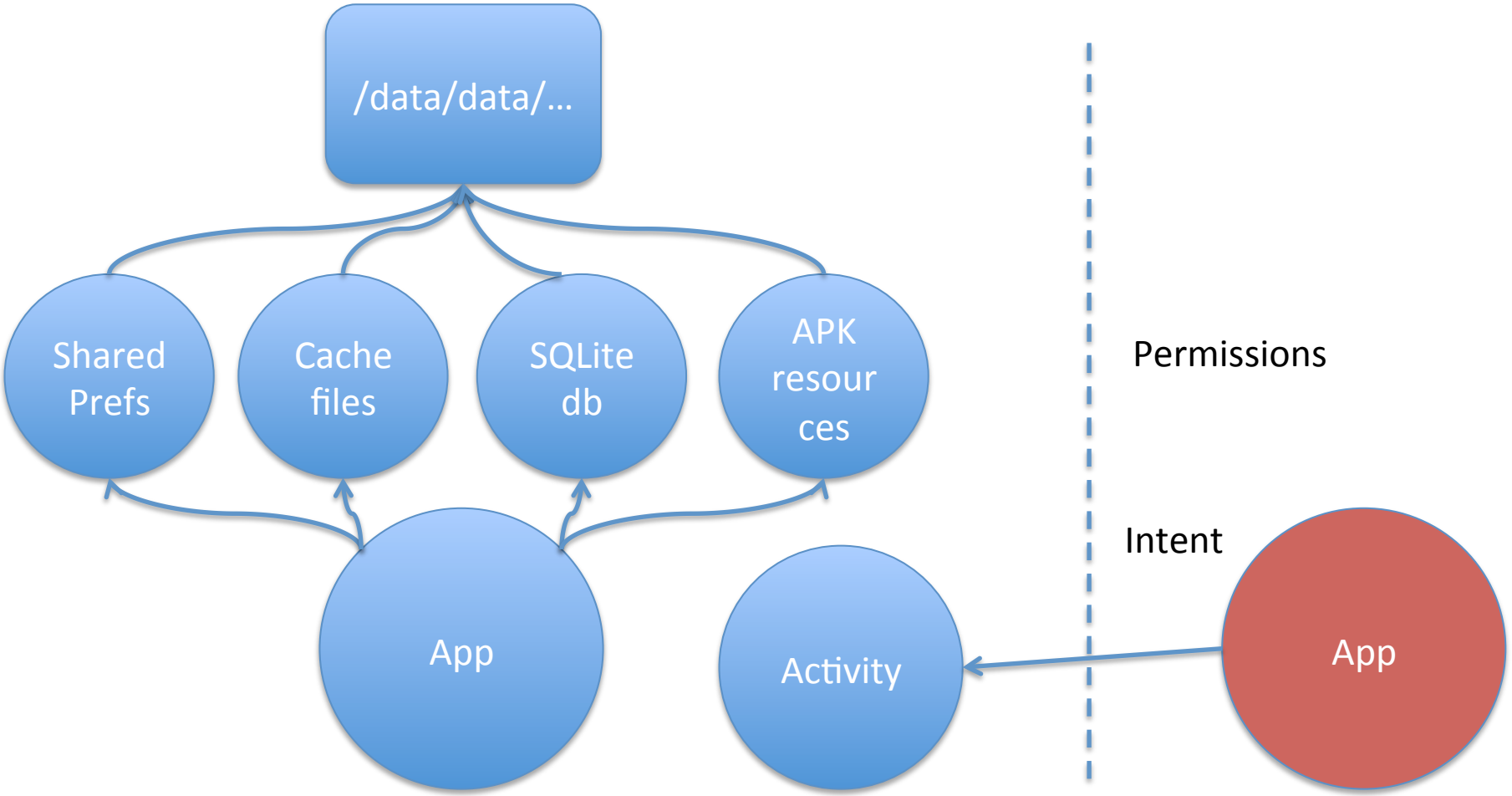
- All of these methods (except onCreate()) take a URI as the first parameter
  - The object will need to parse it to some extent to know what to return, insert or update
  - Android provides android.content.UriMatcher to simplify this
    - Provides mapping between abstraction of contract class to concrete db implementation
  - Does the calling application want all data from a table, or just a row, or a specific table?
    - Or a “virtual” table

Let’s have a look…

Network

- One last type of data storage
  - Get it off the phone, and into the cloud
- Implement a SyncAdapter
  - Appears in the “Accounts and Sync” menu in the OS
  - Synchronizes a local database / content provider with a remote server
  - Make use of a Service to push data in the background
- http://developer.android.com/training/sync-adapters/creating-sync-adapter.html

Sharing Data – is this good enough?

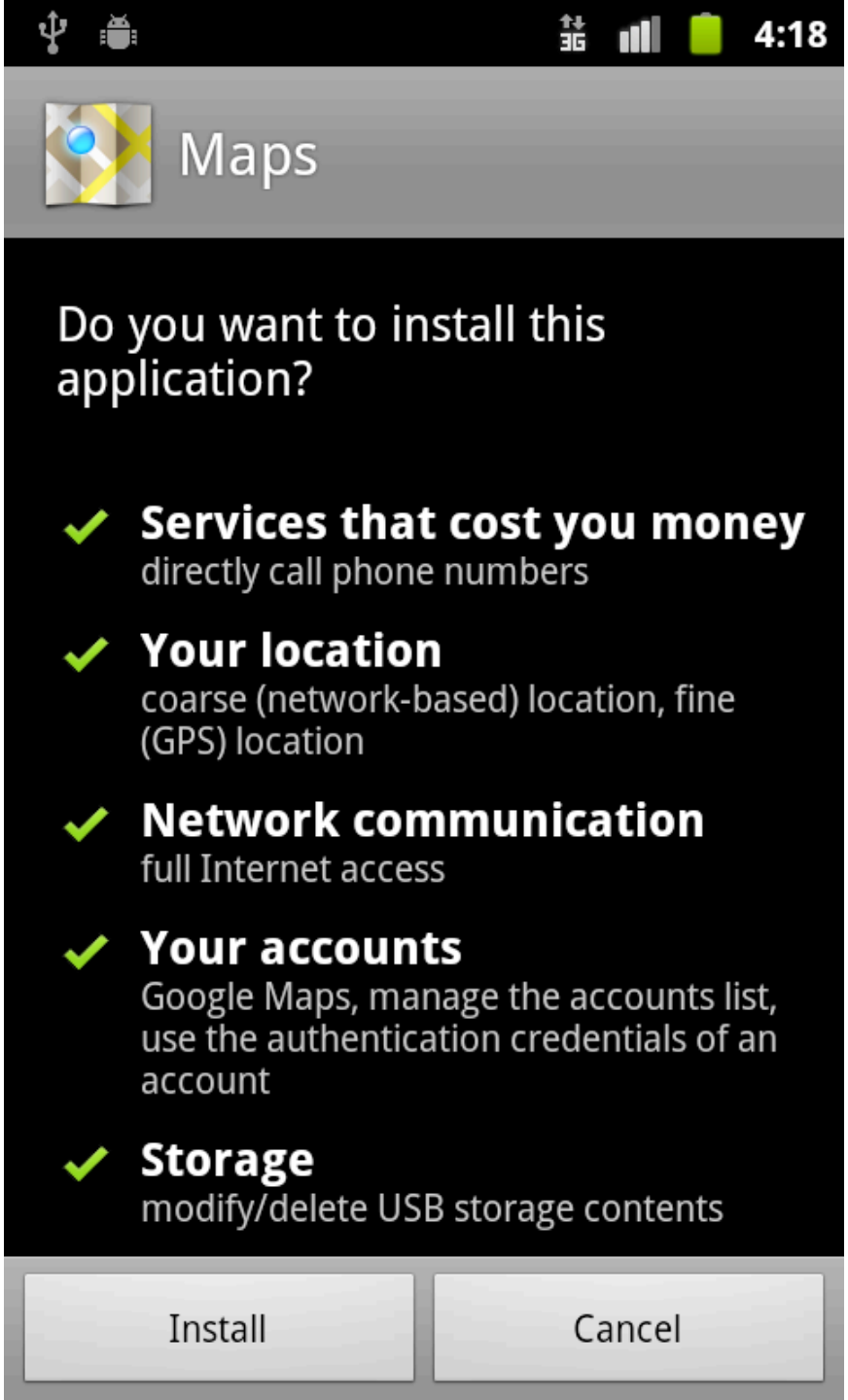


Android Security

- Isolation by default
- Linux kernel
  - Filesystem / UID
    - Private, per-application file storage
  - Processes
    - Individual virtual machine instances
    - Native-code controlled by the application sandbox
- Restricted access to the root user
  - Most processes run as normal users
- IPC through specific interfaces
  - Services, Binders, Intents, Messages, ContentProviders
  - Intentional lack of APIs for sensitive functionality
    - Direct SIM card access

Permissions

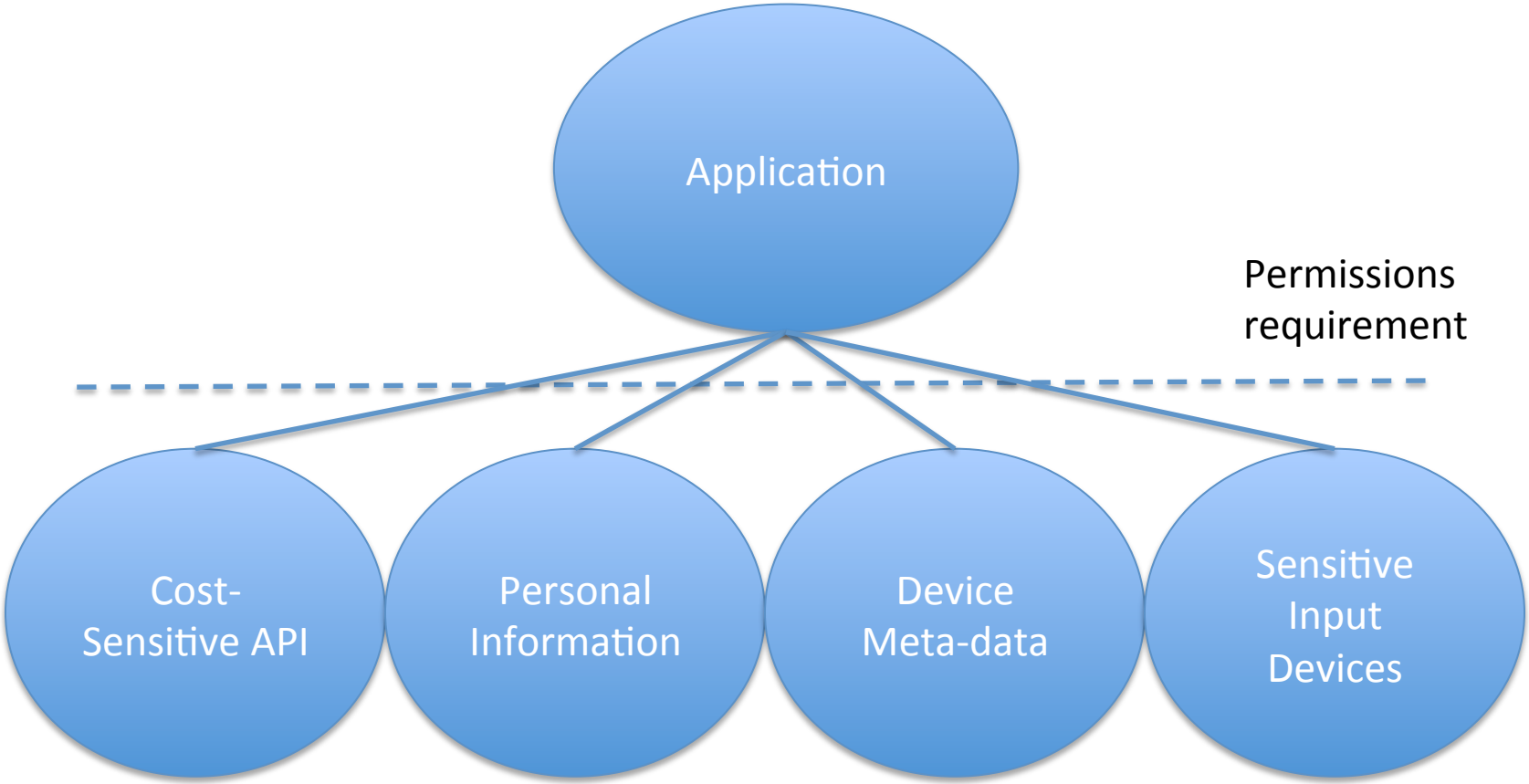
- No access by default
  - Control access to specific mechanisms
- Applications can offer protected access to resources and data with **permissions**
  - Permissions explicitly granted by users
- Permission architecture
  - Applications statically declare permissions
    - Required **of** components interacting with them
      - You must have this permission to interact with me
    - Required **by** components they interact with
      - I will need these permissions
  - Android requires user's consent to specific permissions when an application is installed


4:18
Maps
Do you want to install this application?
Services that cost you money
directly call phone numbers
Your location
coarse (network-based) location, fine (GPS) location
Network communication
full Internet access
Your accounts
Google Maps, manage the accounts list, use the authentication credentials of an account
Storage
modify/delete USB storage contents
Install
Cancel

Permissions

- Show permissions required at install time
  - Not prompted again regarding permissions at run-time
- Why?
  - Not yet made a commitment (financial, mental) to the application
    - Can compare to other applications
  - Not per session / at run-time
    - "Seamless" switching between Activities / applications
    - Would slow down the user experience
    - Train users to click "ok" repeatedly without considering the implications

Permissions



Permissions

- Cost-Sensitive APIs
  - Telephony
  - SMS/MMS
  - Network/Data
  - In-App Billing
  - NFC Access
- Personal Information
  - Contacts, calendar, messages, emails
- Device Meta-data
  - System logs, browser history, network identifiers
- Sensitive Input Devices
  - Interaction with the surrounding environment
  - Camera, microphone, GPS

Common Permissions

- android.permission.ACCESS_FINE_LOCATION
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.INTERNET
- android.permission.WAKE_LOCK

Using Permissions

- Applications can define new permissions in the manifest

  <permission android:name="android.permission.VIBRATE"

  …

  </>

  - Do we really need a new permission?
  - normal / dangerous / signed
  - "Readable" explanation of the new permission
- Applications can require components interacting with them to have a specified permission, set in the manifest
  - By default all permissions apply to all components hosted by the application
    - Activities, Services etc.
  - Or per component permission requirements

Using Permissions

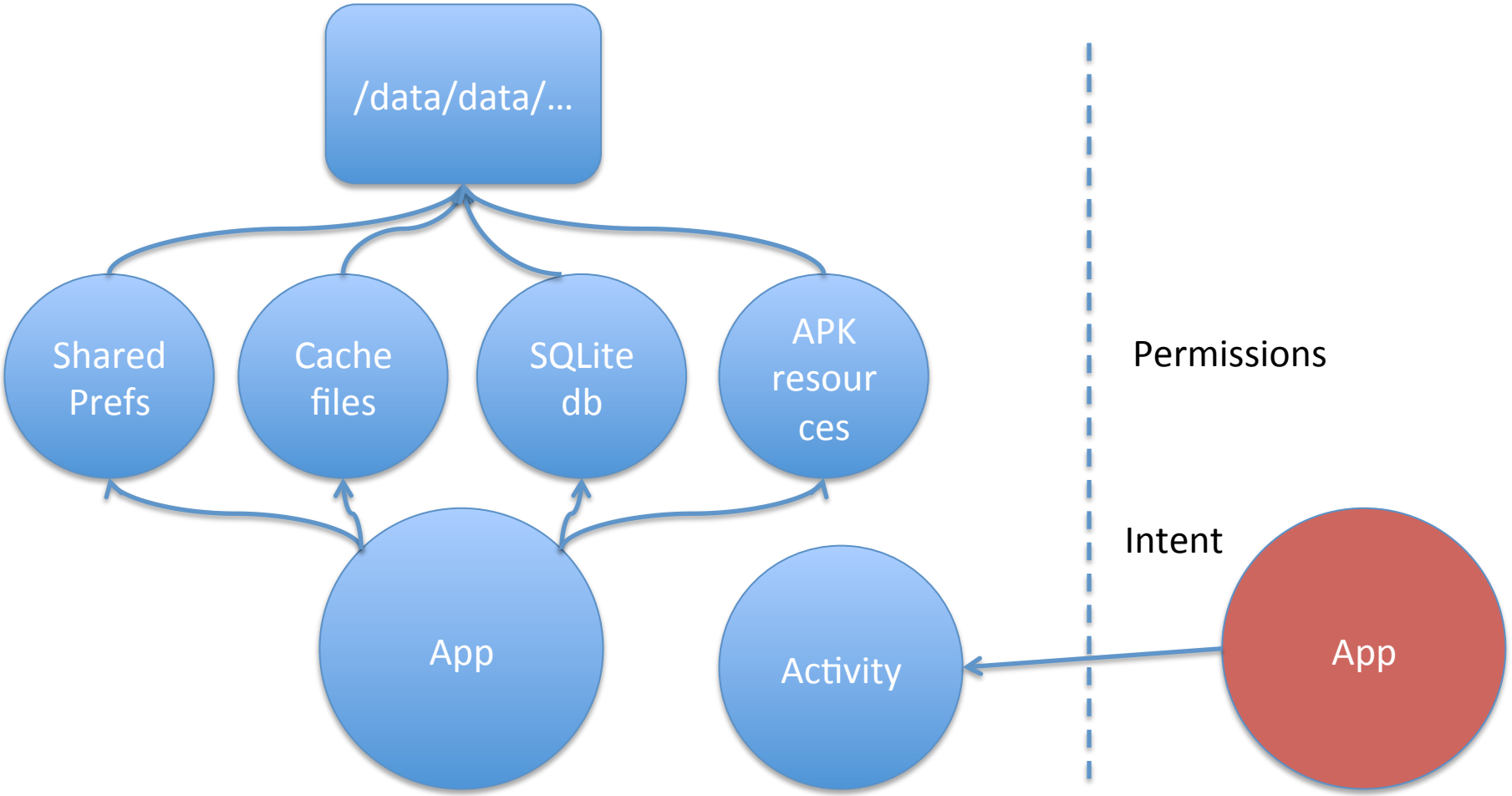
- Specify that an Application **uses** a permission

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

- Specify that an Application **requires** a permission
  - The app must **use** permissions it **requires**

```
<provider
    android:permission="android.permission.READ_CONTACTS”
    android:authorities="com.example.martincontentprovider.MyProvider”
    android:multiprocess="true”
    android:name="com.example.martincontentprovider.MyProvider">
</provider>
```

Sharing Data – is this good enough?



Component Permissions

- Activity
  - Restricts which components can start the activity
  - Checked within execution of:
    - startActivity()
    - startActivityForResult()
- Service
  - Restricts which components can start or bind to the associated service
  - Checked within execution of:
    - Context.startService()
    - Context.stopService()
    - Context.bindService()
- ContentProvider
  - Restricts which components can read or write to a ContentProvider
- Throw SecurityException on permissions failure
  - Usually as we've forgotten to ask for permission during installation

Querying Permissions

- Cannot really ask for more permissions at runtime
- Can query permissions before we try and do something / allow an app to do something
- Does the app using my Service have a permission?
  - Context.checkCallingPermission()
- Does a process have a permission?
  - Context.checkPermission()
- Does an installed app have a permission?
  - PackageManager.checkPermission()

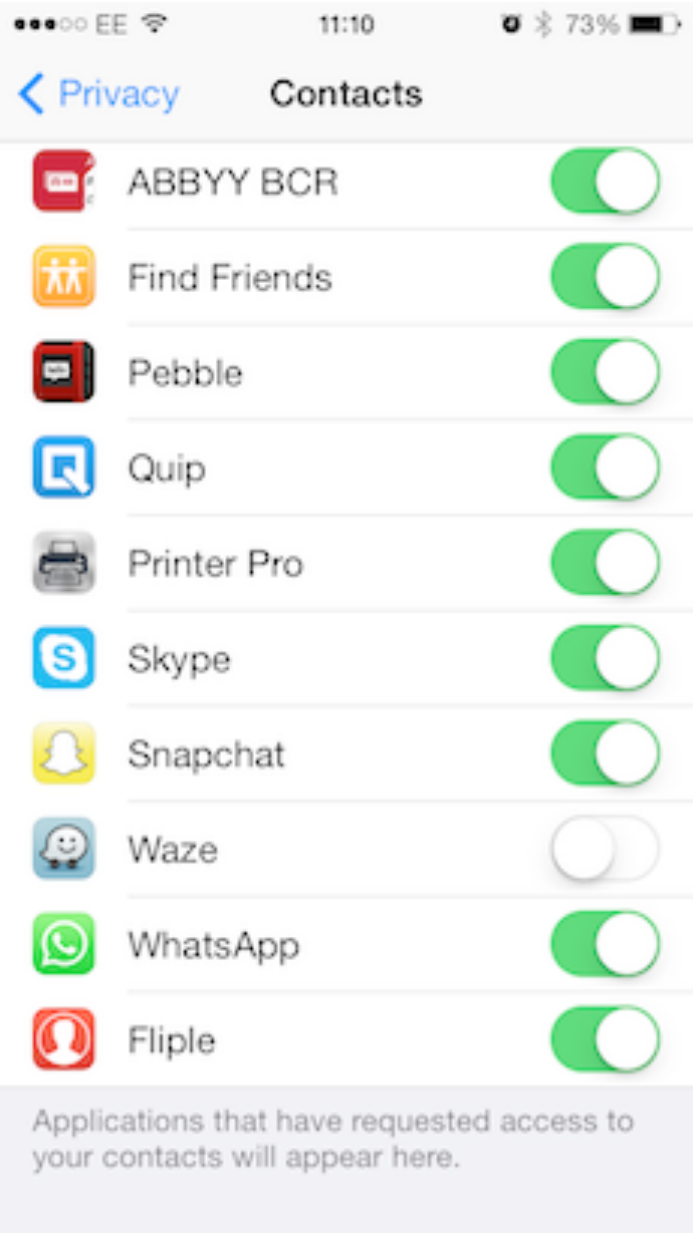
Temporary URI Permissions

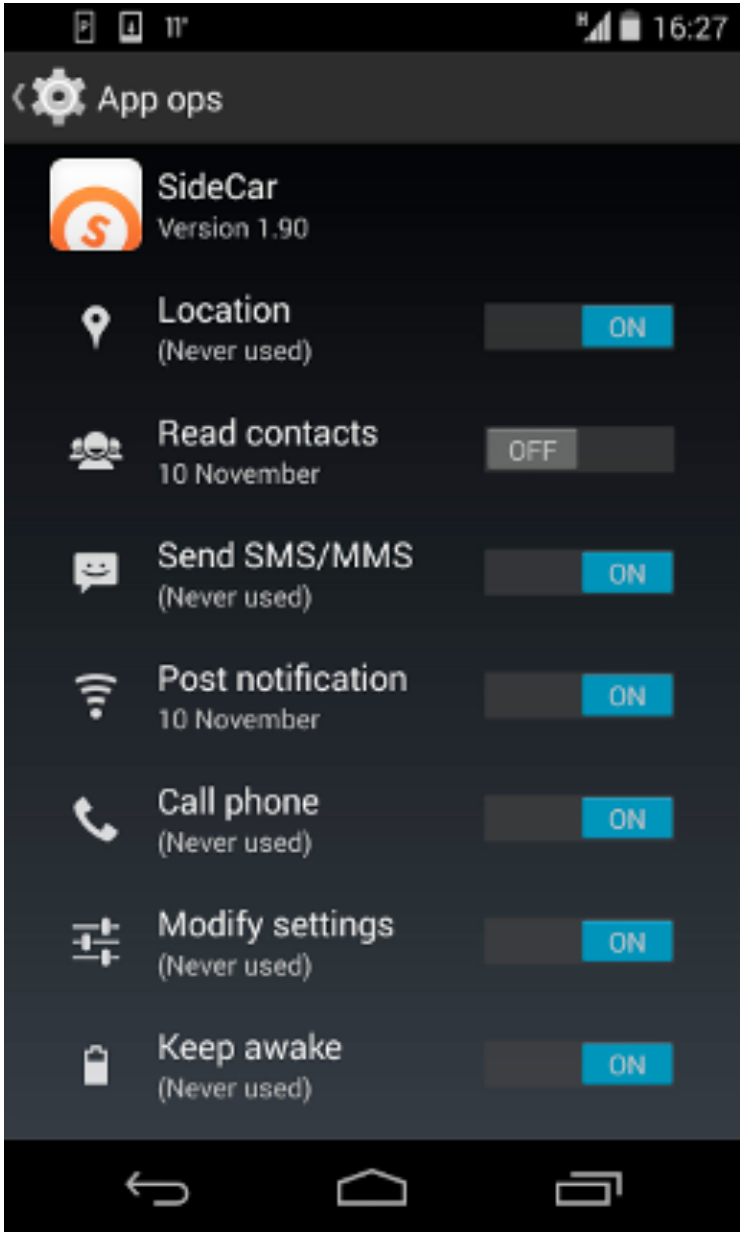
- Applications making use of multiple Activities
  - "Access to the mail should be protected by permissions, since this is sensitive user data. However, if a URI to an image attachment is given to an image viewer, that image viewer will not have permission to open the attachment since it has no reason to hold a permission to access all e-mail."
  - Allow access to specific URIs, not the whole provider

android:grantUriPermissions="true"

myIntent.addFlags(Intent.FLAG_GRANT_READ_URI_PERMISSION);

- Temporary URI permissions last while the stack of the receiving Activity is active


EE
11:10
73%
Privacy
Contacts
ABBYY BCR
Find Friends
Pebble
Quip
Printer Pro
Skype
Snapchat
Waze
WhatsApp
Fliple
Applications that have requested access to your contacts will appear here.


16:27
App ops
SideCar
Version 1.90
Location
(Never used)
ON
Read contacts
10 November
OFF
Send SMS/MMS
(Never used)
ON
Post notification
10 November
ON
Call phone
(Never used)
ON
Modify settings
(Never used)
ON
Keep awake
(Never used)
ON

News › Technology › Android

Android torch app with over 50m downloads silently sent user location and device data to advertisers

US Federal Trade Commission charges 'deception' over app which turned on lights on Android smartphones - but also told advertisers about location and device information

Permissions in the wild

- Study participants displayed low attention and comprehension rates: both the Internet survey and laboratory study found that 17% of participants paid attention to permissions during installation, and only 3% of Internet survey respondents could correctly answer all three permission comprehension questions.
- http://dl.acm.org/citation.cfm?id=2335360

Permissions vs Use

- Read your text messages
  - To confirm your phone number via text message (if you've added it to your account)
- Read/write contacts
  - To import and sync your phone's contacts to Facebook, or vice versa (think updating contact images)
- Add and/or modify calendar events and send emails to guests without your knowledge
  - To see your Facebook events in your phone's calendar
- Read calendar events plus confidential information
  - To check your calendar for you to see if you have something already scheduled for the time of the Facebook event you're currently viewing

References

- http://developer.android.com/guide/topics/providers/content-providers.html
- http://developer.android.com/guide/components/fundamentals.html