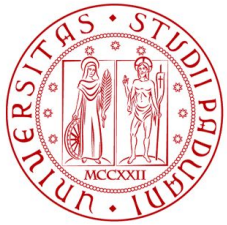
Mobile Security

Dr. Eleonora Losiouk
Department of Mathematics
University of Padua
elosiouk@math.unipd.it
https://www.math.unipd.it/~elosiouk/

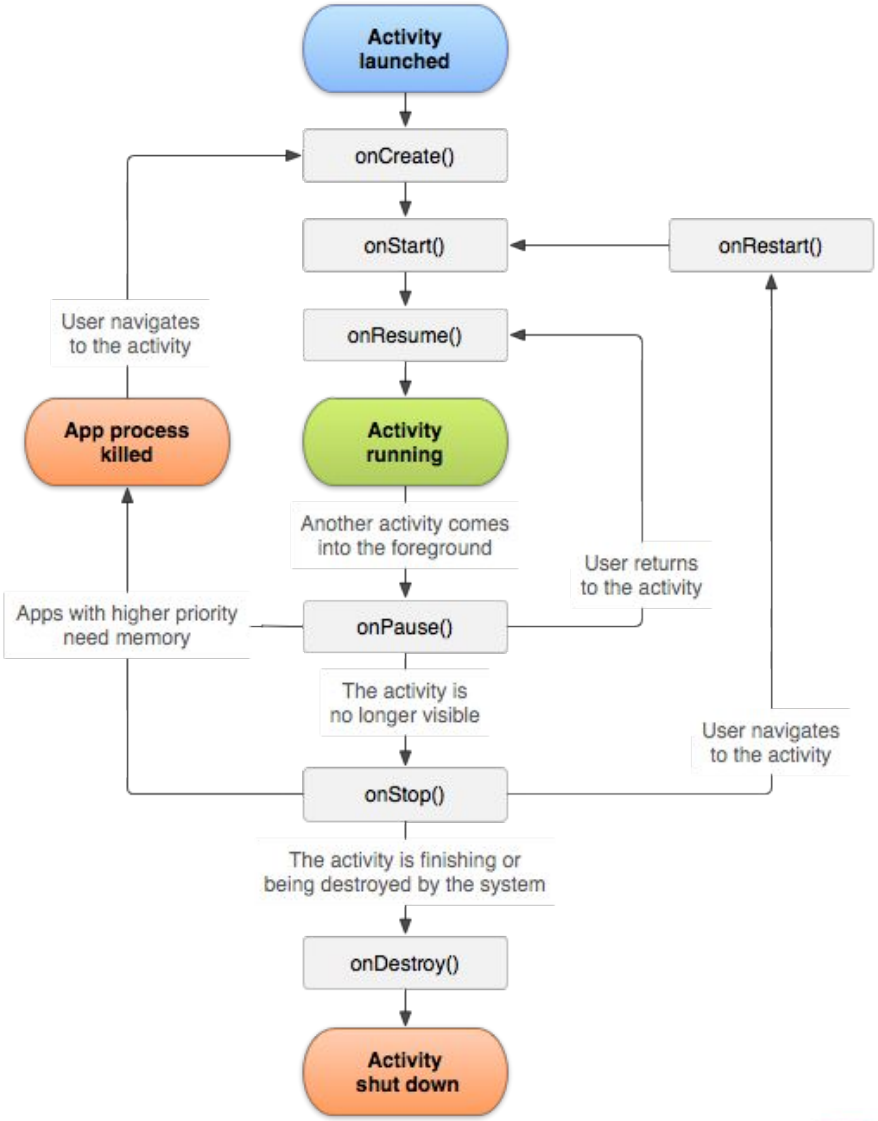


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

DIPARTIMENTO
MATEMATICA

Activities


Activity launched
onCreate()
onStart()
onRestart()
onResume()
Activity running
User navigates to the activity
App process killed
Another activity comes into the foreground
User returns to the activity
Apps with higher priority need memory
onPause()
The activity is no longer visible
User navigates to the activity
onStop()
The activity is finishing or being destroyed by the system
onDestroy()
Activity shut down

Activities

- To start an activity
  - startActivity(intent)
  - intent can be either explicit or implicit

- New: activities can also get an "answer" / "result"

Activities

- To start an activity
  - startActivity(intent)
  - intent can be either explicit or implicit

- New: activities can also get an "answer" / "result"

A.X

```
Intent i = new Intent(...);
int requestCode = 400;
startActivityForResult(i,
requestCode);
```

B.Y

```
onCreate() {
  Intent resInt = new Intent();
  ...
  setResult(Activity.RESULT_OK,resInt);
  finish();
}
```

Activities

- To start an activity
  - startActivity(intent)
  - intent can be either explicit or implicit

- New: activities can also get an "answer" / "result"

A.X

```
Intent i = new Intent(...);
int requestCode = 400;
startActivityForResult(i,
requestCode);
```

B.Y

```
onCreate() {
  Intent resInt = new Intent();
  ...
  setResult(Activity.RESULT_OK,resInt);
  finish();
}
```

```
onActivityResult(int requestCode, int resultCode, Intent data) {
  // check requestCode and resultCode
  ...
}
```

Services

- Three types of services:
  - Background
  - Foreground
  - Bound

- Full docs: link

Services

- To start a service
  - Intent i = new Intent(...);
  - intent MUST be an explicit intent (for security reasons)
  - startService(i)

- How to get back a reply?
  - No analogous of startActivityForResult
  - There are some ways, but the easiest is via broadcast intents

Why not a problem for activities?
Chooser dialog!

Background Services

- It performs an operation that isn't directly noticeable by the user
- Start with startService()
- startService() → S.onCreate() → S.onStartCommand()

Foreground Services

- It performs an operation that is noticeable to the user
- Start with startService() + startForeground() (from the service's onCreate)
- startService() → S.onCreate() → S.onStartCommand()

Bound Services (doc)

- A service is bound when an app *binds* to it by calling bindService()
- You can have client/server IPC-based interaction
- bindService() → S.onCreate() → S.onBind()

Three Ways of Implementing Services

- Local Service (intra-app)
- Using a Messenger
- Using AIDL

Bound Services

- Client → service communications
- If the service needs to send back a message, the client needs to create a Messenger in the client.
- Have fun: link

Broadcast Intents and Receivers

- To send an intent around the system aka "broadcast"
  - sendBroadcast(intent)
- Relevant broadcast receivers will be woken up

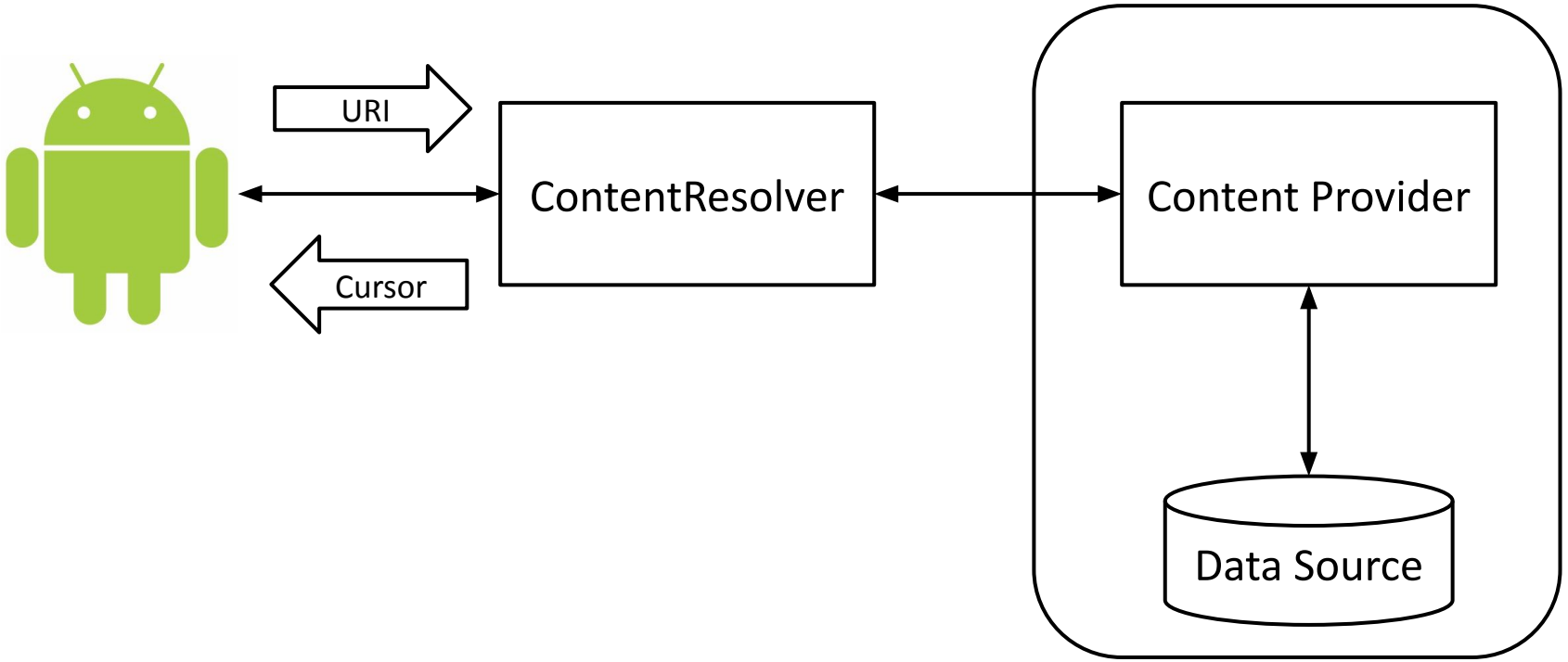
Broadcast Receiver "registration"

- Via manifest + intent filter
- At run-time (only for broadcast receivers!)

```
MyReceiver customRec = new MyReceiver();
IntentFilter intFil = new IntentFilter("com.some.action");
registerReceiver(customRec, intFil);
```

Content Provider

- Sometimes it is required to share data across applications. This is where content providers become very useful



Android's Built-in Content Providers

- Browser
  - Browser bookmarks, browser history
- CallLog
  - Missed calls, call details
- Contacts
  - Contact details
- MediaStore
  - Media files
- Settings
  - Device settings and preferences

adb shell content query --uri content://com.android.contacts/contacts

How to Make an App's Data Public?

- Two options
  - You can create your own content provider (extending ContentProvider class) or
  - You can add the data to an existing provider — if there's one that controls the same type of data and you have permission to write to it

How to Make an App's Data Public?

- Two options
  - You can create your own content provider (extending ContentProvider class) or
  - You can add the data to an existing provider — if there's one that controls the same type of data and you have permission to write to it
- All content providers implement a common interface for
  - Querying the provider and returning results
  - Adding
  - Altering
  - Deleting
- How a content provider actually stores its data under the cover is up to its designer

Data Model

- Content providers expose their data as a simple table (like in a database) model
  - Each row is a record and each column is data of a particular type and meaning
  - Every record includes a numeric _ID field that uniquely identifies the record within the table

Data Model

- Content providers expose their data as a simple table (like in a database) model
  - Each row is a record and each column is data of a particular type and meaning
  - Every record includes a numeric _ID field that uniquely identifies the record within the table

content://	com.android.contacts/	contacts/	100

What a Query Returns

- A query returns a set of zero or more records
- The retrieved data is exposed by a Cursor object that can be used to iterate backward or forward through the result set
  - You can use Cursor object only to read the data
  - To add, modify, or delete data, you must use a ContentResolver object