Introduction to Android

Elias Athanasopoulos
FORTH
elathan@ics.forth.gr

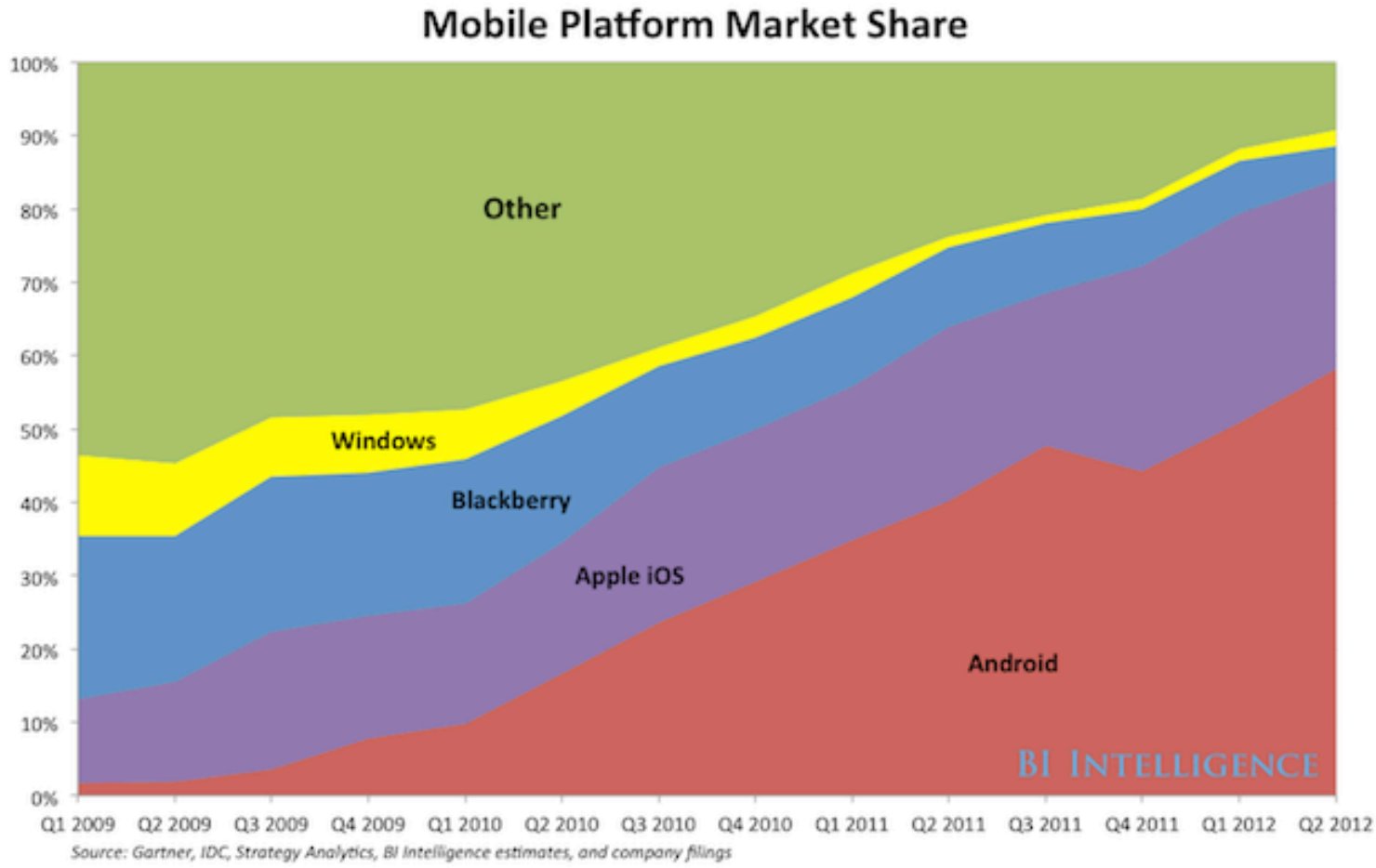
Bird's Eye View

- What is Android?
- Bootstrap
- Short walk to the tools
- Android permission model

What is Android?

- Linux-based Operating System
- Designed primarily for mobile devices
  - Power constraints
  - Sensor rich
- Combines technologies from other OSs
  - Binder for IPC

Android popularity



"By the end of **2016**, there will be **2.3 billion** computers, tablets and smartphones running **Android**, and only **2.28 billion Windows-powered devices**, says research firm **Gartner**." ***ZDNet.com***

In other words…

- More devices
- More users
- More data
- Bigger attack landscape

Application Stores

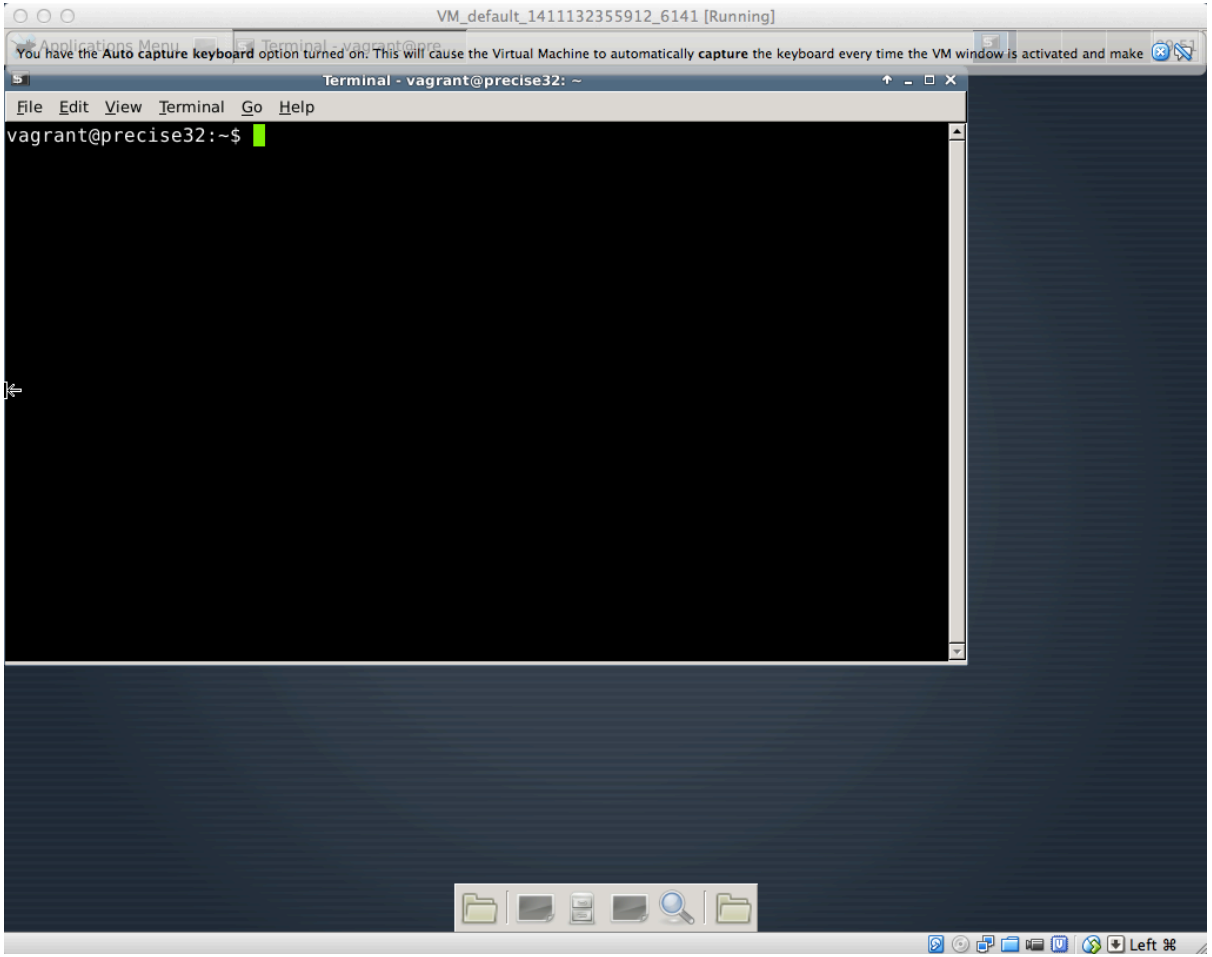
Bootstrap – Let's see how it looks

Step 1 – Downloads

- VirtualBox
  - A virtual machine software
- Vagrant
  - A utility for creating portable images
- An image prepared by us
  - Ubuntu with Android SDK/tools
  - Android emulator

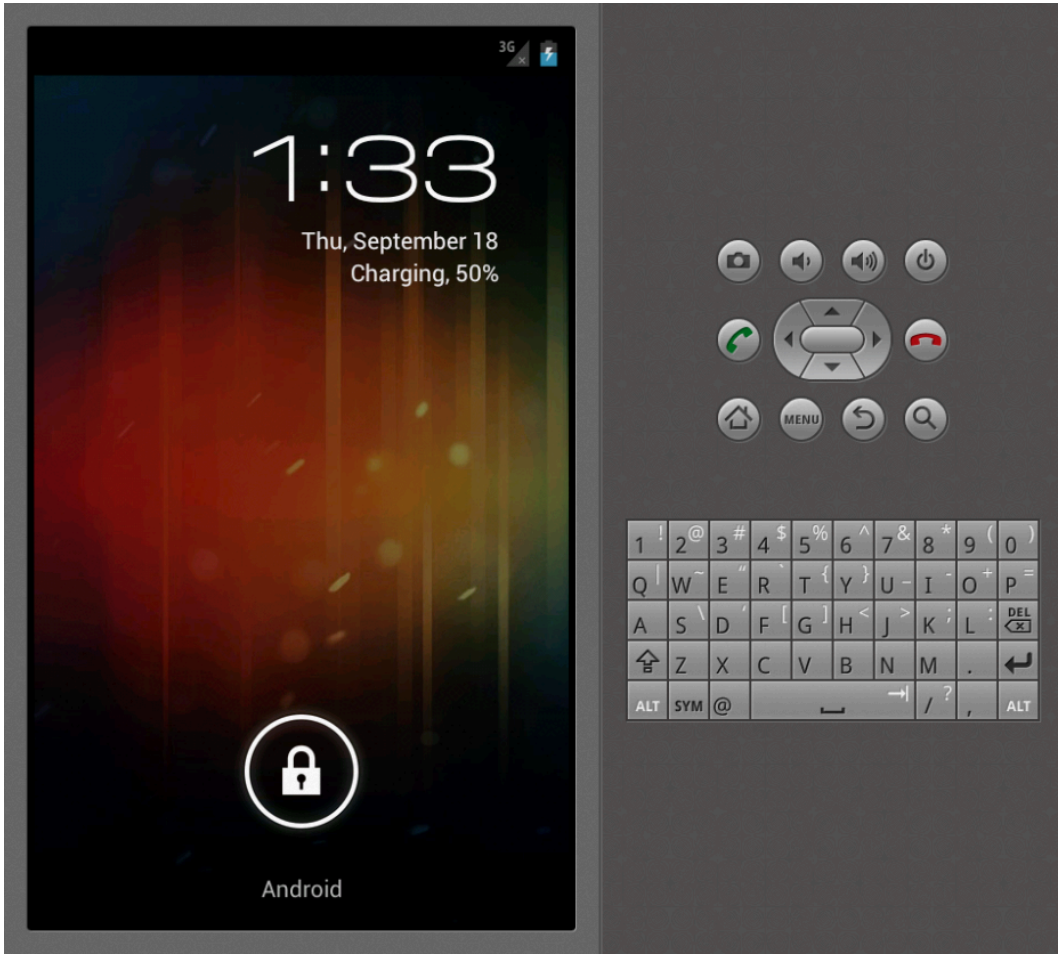
Log in to the environment

- Run VirtualBox with our image
  - `login: vagrant`
  - `password: vagrant`
  - `% startxfce4`
  - Run a terminal


VM_default_1411132355912_6141 [Running]
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make
Terminal - vagrant@precise32: ~
File Edit View Terminal Go Help
vagrant@precise32:~$
Left ⌘

Run the emulator

- Create a new emulator environment
  - `% android list targets`
  - `% android create avd –n syssec –t 1 --abi default/armeabi`
- Run the emulator
  - `% emulator @syssec`
  - `% adb shell`


3G
1:33
Thu, September 18
Charging, 50%
Android
MENU

Create external storage

```
% mksdcard -l e 12M syssec-sd.img
% emulator @syssec –sdcard syssec-sd.img
```

Moving files around

```
% echo “Hello Android” > hello.txt
% adb push hello.txt /sdcard/
% adb shell
# cat /sdcard/hello.txt
Hello Android
```

Read-only filesystem?

- Mount external storage as read/write:

```
# mount –o remount, rw /sdcard
```

Moving files around

```
# cd /sdcard
# echo “Hello from Android” >
hello2.txt
# exit
% adb pull /sdcard/hello2.txt
% cat hello2.txt
Hello from Android
```

Installing/uninstalling apps

```
% cd apps/session1
% adb install
uk.co.nickfines.RealCalc.apk
% adb uninstall
uk.co.nickfines.RealCalc
```

Android Permission Model

- Android powers devices with many resources
  - Sensors: Camera, GPS, Accelerometer, etc.
  - System resources: Network, Storage, etc.
  - Social resources: Contacts, AddressBook, etc.
  - Cellular resources: phone calls, SMSs, etc.

Android Permission Model

- Android is application centric
  - Android apps run in isolation
  - Each app is “a user” (uid) in the system
  - Each app (i.e., user) has access to a set of particular resources

Android Permission Model

- An example (what does the following do?):

```
<manifest xmlns:android=
http://schemas.android.com/apk/res/android
package="com.android.app.myapp">
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
...
</manifest>
```

Many Permissions

String	ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.
String	ACCESS_LOCATION_EXTRA_COMMANDS	Allows an application to access extra location provider commands
String	ACCESS_MOCK_LOCATION	Allows an application to create mock location providers for testing
String	ACCESS_NETWORK_STATE	Allows applications to access information about networks
String	ACCESS_SURFACE_FLINGER	Allows an application to use SurfaceFlinger's low level features.
String	ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks
String	ACCOUNT_MANAGER	Allows applications to call into AccountAuthenticators.
String	ADD_VOICEMAIL	Allows an application to add voicemails into the system.
String	AUTHENTICATE_ACCOUNTS	Allows an application to act as an AccountAuthenticator for the AccountManager
String	BATTERY_STATS	Allows an application to collect battery statistics
String	BIND_ACCESSIBILITY_SERVICE	Must be required by an `AccessibilityService`, to ensure that only the system can bind to it.
String	BIND_APPWIDGET	Allows an application to tell the AppWidget service which application can access AppWidget's data.
String	BIND_DEVICE_ADMIN	Must be required by device administration receiver, to ensure that only the system can interact with it.
String	BIND_INPUT_METHOD	Must be required by an `InputMethodService`, to ensure that only the system can bind to it.
String	BIND_NFC_SERVICE	Must be required by a `HostApduService` or `OffHostApduService` to ensure that only the system can bind to it.

Where permissions are defined?

- Android apps come in bundles
  - APKs (compressed)
- Each app has an AndroidManifest.xml
  - XML file (compressed)

Analyzing an APK with apktool

```
% cd apps/session1
% apktool d
uk.co.nickfines.RealCalc.apk
realcalc
% cd realcalc
% cat AndroidManifest.xml | less
```

Challenge time!