Android “OS” Internals

Prabhaker Mateti
A first glimpse of Android Internals
Android Version History

Android System

• Open software platform for mobile devices
• A complete stack – OS, Middleware, Applications
• An Open Handset Alliance (OHA) project
• Powered by Linux OS
• Application development mostly in Java
• Open source under the Apache 2 license
Device Characteristics

- CPU: ARM 500-2600 Mhz; recently Intel Atom
- RAM available to an App is not as much as on PCs
- “Disk” (flash) access is slow cf to HDD/SSD
- Lifecycle: Apps must pause/quit often, and restore to give the illusion that they are always running
- UI design
  - screen may be HVGA (320x480) to 1920x1080 to ...
  - may be in portrait (h > w) or landscape (w > h)
  - high DPI -- small text may not be readable
  - touch resolution is low (~25 pixel)
- Network access may be slow and intermittent
Std kernel parts not shown
Linux OS Inside

- Linux Kernel Works as a HAL
- Linux/Android Device drivers
- Linux Memory management
- Linux Process management
- Linux Networking
- Kernel from the Linux FOSS project
Android Runtime
Android Java

- Java syntax is the same. But, not all libs are included.
- Unused: Swing, AWT, SWT, lcmdgui
- Android Java = Java SE – AWT/Swing + Android API
Dalvik Virtual Machine

• Dalvik VM is a new JVM by Google
  – Register-based versus stack-based JVM
  – Different set of Java libraries than JDK
• Dalvik VM has been optimized for mobile devices
  – not so powerful CPU
  – memory shortage
  – Dalvik Executable .dex format is compact
  – run multiple VMs efficiently.
Dalvik Virtual Machine (Contd)

• Can have JIT enabled
• Relying on the Linux Kernel for:
  – Threading
  – Low-level memory management
• Projects for making JRuby, Groovy, and Scala first class languages for Android.
Art Virtual Machine

• Android Run Time (ART) libart.so
• Replaces Dalvik libdvm.so (starting with 4.5?)
• Faster And Battery improvements
• https://source.android.com/devices/tech/dalvik/art.html
Libraries

• Surface Manager: A compositing window manager similar to Compiz. Instead of drawing directly to the screen buffer, drawing commands go into off-screen bitmaps that are then combined with other bitmaps to form the display the user sees. Can create see-through windows, fancy transitions, ...

• 2D and 3D graphics: Use 3D hardware or a software renderer. OpenGL.

• Media codecs: AAC, AVC (H.264), H.263, MP3, MPEG-4, ...
Libraries

• Browser engine:
  – WebKit library for rendering web pages
  – the same engine used in KDE, the Google Chrome browser, Apple’s Safari browser, the iPhone, and Symbian 60.
OpenGL ES Momentum

• The leading 3D rendering API for mobile and embedded devices
  - Based on desktop OpenGL – but optimized for mobile / handheld devices
  - Removes redundancy & rarely used features - adds mobile-friendly data types
  - The power of OpenGL distilled into a much smaller package

• OpenGL ES adopted by every major handset OS
  - Pervasive mobile 3D is evolving fast

• OpenGL ES has become the most widely deployed 3D API
  - Used in diverse applications, devices and markets
  - Mobile phones, games consoles, personal navigation devices, personal media players
  - Automotive systems, settop boxes
OpenGL ES

• OpenGL ES is a subset of OpenGL graphics standard.
• OpenGL ES is a ... low-level interface between software and graphics acceleration. OpenGL ES includes profiles for floating-point and fixed-point systems and the EGL™ specification ....
• OpenGL ES 1.X is for fixed function hardware and offers acceleration, image quality and performance.
• OpenGL ES 2.X enables full programmable 3D graphics.
• http://www.khronos.org/opengles/
SQLite

• SQLite database engine
  – Provides persistent storage.
  – Also used in Firefox and the iPhone.
  – android.database.sqlite

• Application would use to manage its own private database.
• /system/xbin/sqlite3
Background: What is a program?

• (Will add more details based on feedback.)
• Precise def will be based on OS.
• Do NOT use “program” and “process” interchangeably.
• A program is a file
  – Executable permissions
  – Structure of content rigidly defined by an executable formats
    • Linux: ELF, a.out, coff
    • Windows: com, exe
    • Java: .class files
    • Android: .dex
• Program v Object code files
  – generated by a linker
  – On Linux, /usr/bin/Id (historically misnamed)
  – The compiler/IDE tool chain invokes the linker
• APK file includes
  – the .dex file
  – along with other files describing resources.
• “App” is an alternate term for a program
Background: What is a process?

- Process is a run-time volatile entity created by an OS system call `exec`.
- Processes have a virtual memory footprint:
  - Code (machine instructions)
  - Run time stack content
  - Run time heap content
  - Run time global variables
- Subject to paging and swapping.
- Android details are more complex cf. Linux.
Selected root Processes

• The following examples are typical
• % ps | wc –l was 220

root  1  /init
root  1835  /system/bin/vold
root  1838  /system/bin/netd
root  1839  /system/bin/debuggerd
root  1840  /system/bin/sh
root  1848  zygote
root  2479  kcryptd

• URL ps-full-list.txt
Selected system+ Processes

• system 1834 /system/bin/servicemanager
• system 1847 /system/bin/surfaceflinger
• gps 1855 /system/bin/gpsd
• media_rw 1880 /system/bin/sdcard
• system 2775 com.sec.android.inputmethod
• system 2824 com.sec.android.app.snotebook
• wifi 3420 /system/bin/wpa_supplicant
• dhcp 3533 /system/bin/dhcpcd
• radio 2798 com.android.phone
Selected user Processes

- u0_a126  2656  com.android.systemui
- u0_a16   2909  com.google.process.gapps
- u0_a6    3110  android.process.acore
- u0_a16   3162  com.google.process.location
- u0_a6    3857  com.android.contacts
- u0_a101  3906  com.sec.phone
- u0_a77   4979  com.android.vending
- u0_a203  5535  org.mozilla.firefox
- u0_a236  5723  com.twitter.android
- u0_a162  7604  com.kk.launcher
- u0_a189  8461  com.devexpert.weather
- u0_a112  12143 com.sec.android.app.music
- u0_a58   12199 com.samsung.music
- u0_a226  12230 com.android.chrome
- u0_a25   29235 android.process.media

First column is user names
File System

- ext3, ext4 of Linux
- Mount points
  - One for system, one for the apps, and one for whatever.
- Each app has its own sandbox accessible to it. No one else can access its data.
- /sdard
- /mnt/extSdCard
Partitions

• Example: Samsung T679
  – ARMv7 (v7l)
  – fdisk -l /dev/ block/ mmcblk0
  – lists 37 partitions.

<table>
<thead>
<tr>
<th>Path</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/block/mmcblk0p15</td>
<td>/system</td>
</tr>
<tr>
<td>/dev/block/mmcblk0p16</td>
<td>/cache</td>
</tr>
<tr>
<td>/dev/block/mmcblk0p</td>
<td>/data</td>
</tr>
<tr>
<td>/dev/block/vold/179:33</td>
<td>/storage/sdcard1</td>
</tr>
<tr>
<td>/dev/block/vold/179:28</td>
<td>/storage/sdcard0</td>
</tr>
</tbody>
</table>
### Filesystem Sizes

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Free</th>
<th>Blksizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev</td>
<td>916.3M</td>
<td>128.0K</td>
<td>916.2M</td>
<td>4096</td>
</tr>
<tr>
<td>/sys/fs/cgroup</td>
<td>916.3M</td>
<td>12.0K</td>
<td>916.3M</td>
<td>4096</td>
</tr>
<tr>
<td>/mnt/asec</td>
<td>916.3M</td>
<td>0.0K</td>
<td>916.3M</td>
<td>4096</td>
</tr>
<tr>
<td>/mnt/obb</td>
<td>916.3M</td>
<td>0.0K</td>
<td>916.3M</td>
<td>4096</td>
</tr>
<tr>
<td>/mnt/fuse</td>
<td>916.3M</td>
<td>0.0K</td>
<td>916.3M</td>
<td>4096</td>
</tr>
<tr>
<td>/system</td>
<td>826.8M</td>
<td>713.1M</td>
<td>113.7M</td>
<td>4096</td>
</tr>
<tr>
<td>/cache</td>
<td>551.2M</td>
<td>10.1M</td>
<td>541.1M</td>
<td>4096</td>
</tr>
<tr>
<td>/data</td>
<td>5.7G</td>
<td>3.9G</td>
<td>1.8G</td>
<td>4096</td>
</tr>
<tr>
<td>/persist</td>
<td>15.7M</td>
<td>4.1M</td>
<td>11.6M</td>
<td>4096</td>
</tr>
<tr>
<td>/firmware</td>
<td>64.0M</td>
<td>44.4M</td>
<td>19.5M</td>
<td>16384</td>
</tr>
<tr>
<td>/mnt/shell/emulated</td>
<td>5.7G</td>
<td>3.9G</td>
<td>1.8G</td>
<td>4096</td>
</tr>
</tbody>
</table>

(My rooted Nexus 4, May 2014)
Commands

• /system/bin
  – mount, swap, top, adb
  – blkid, bootanimation
  – backuptool.sh
  – bugreport
  – chmod, chown
  – du, e2fsck, fsck.exfat
  – gdbserver, grep, gzip
  – iptables, kill
  – ssh*, top, ps

• /system/xbin
  – busybox
  – crond
  – dd, df, fdisk, tune2fs
  – nanddump
  – nslookup
  – nice
  – pidof, pkill, pwd
  – strace, su, sync, sha1sum
  – zip
ls -l /proc/1 (trimmed)

```
-rw------- root     root            0 2014-05-12 06:39 attr
-r--r--r-- root     root            0 2014-05-11 22:43 cmdline
lrwxrwxrwx root     root              2014-05-12 06:39 cwd -> /
-r-------- root     root            0 2014-05-12 06:39 environ
lrwxrwxrwx root     root              2014-05-12 06:39 exe -> /init
dr-x------ root     root              2014-05-12 06:39 fd
dr-x------ root     root              2014-05-12 06:39 fdinfo
-r-------- root     root            0 2014-05-12 06:39 io
-r--r--r-- root     root            0 2014-05-12 06:39 limits
-rw-r--r-- root     root              2014-05-12 06:39 loginuid
-r--r--r-- root     root            0 2014-05-12 06:39 maps
-rw------- root     root            0 2014-05-12 06:39 mem
-r--r--r-- root     root            0 2014-05-12 06:39 mountinfo
-r--r--r-- root     root            0 2014-05-12 06:39 mounts
-r-------- root     root            0 2014-05-12 06:39 mountstats
dr-x--x--x root     root              2014-05-12 06:39 ns
-r--r--r-- root     root            0 2014-05-12 06:39 pagemap
-r--r--r-- root     root              2014-05-12 06:39 personality
lrwxrwxrwx root     root              2014-05-12 06:39 root -> /
-r--r--r-- root     root            0 2014-05-12 06:39 sessionid
-r--r--r-- root     root            0 2014-05-12 06:39 smaps
-r--r--r-- root     root            0 2014-05-12 06:39 stack
-r--r--r-- root     root            0 2014-05-11 22:43 stat
-r--r--r-- root     root            0 2014-05-12 06:39 statm
-r--r--r-- root     root            0 2014-05-11 22:45 status
-r--r--r-- root     root            0 2014-05-12 06:39 wchan
```
Android Hardware Abstraction (HAL)

- Linux originated
  - /dev/zero, /dev/null
  - /dev/random
  - /dev/input/*
  - /dev/tty
  - /dev/kmem
  - /sys/dev/block
- Mfr specific details abstracted out
  - All cameras, GPS, ...
- Example /dev entries
  - Video
  - msm_camera
  - msm_dsp
  - msm_rotator
  - msm_vidc_dec
  - wcns_wlan
IPC Mechanism in Android

• In GNU/Linux
  – Pipes
  – Shared Memory
  – Message Queue

• In Android
  – Binder
App Runtime Service
Android Application

Linux Process

DB

Prefs

File System
Performance

- Avoid static methods
  - they're much faster
  - call takes longer time
- Use native methods
  - internal getters/setters
- Avoid enums
- Avoid floating-point operations
  - no hardware support
- Cache field lookups
  - int count = this.mCount;
  - Item[] items = this.mItems;
  - for (int i = 0; i < count; i++)
  - dumpItems(items[i]);
- Use static keyword
  - Avoid creating objects
    - methods do not change state of object
    - final for constants
Application Security

• Each Android application
  – own Linux process.
  – own userid.
  – own sandbox file system
  – own set of preferences
  – own database.

• Other applications cannot access any of its data, unless it is explicitly shared.

• finer-grained security features through a "permission" mechanism

• per-URI permissions for granting ad-hoc access

• More later
/system/etc/permissions/...

- android.hardware.camera.front.xml
- android.hardware.sensor.gyroscope.xml
- android.hardware.telephony.gsm.xml
- android.hardware.usb.host.xml
- android.hardware.wifi.xml
- com.cyanogenmod.android.xml
- features.xml
- platform.xml
How to Explore Android Internals

• Install a “terminal” app. If your device is rooted, you can change things. (We will discuss “root” later.)

• adb shell

• Install an ssh server on the Android device, and from Linux ssh into it.
  – Highly useful.
  – E.g., filezilla sftp client invoked on Linux
  – Some devices already have /system/bin/sshd
References

• Karim Yaghmour, Embedded Android book