Android Internals

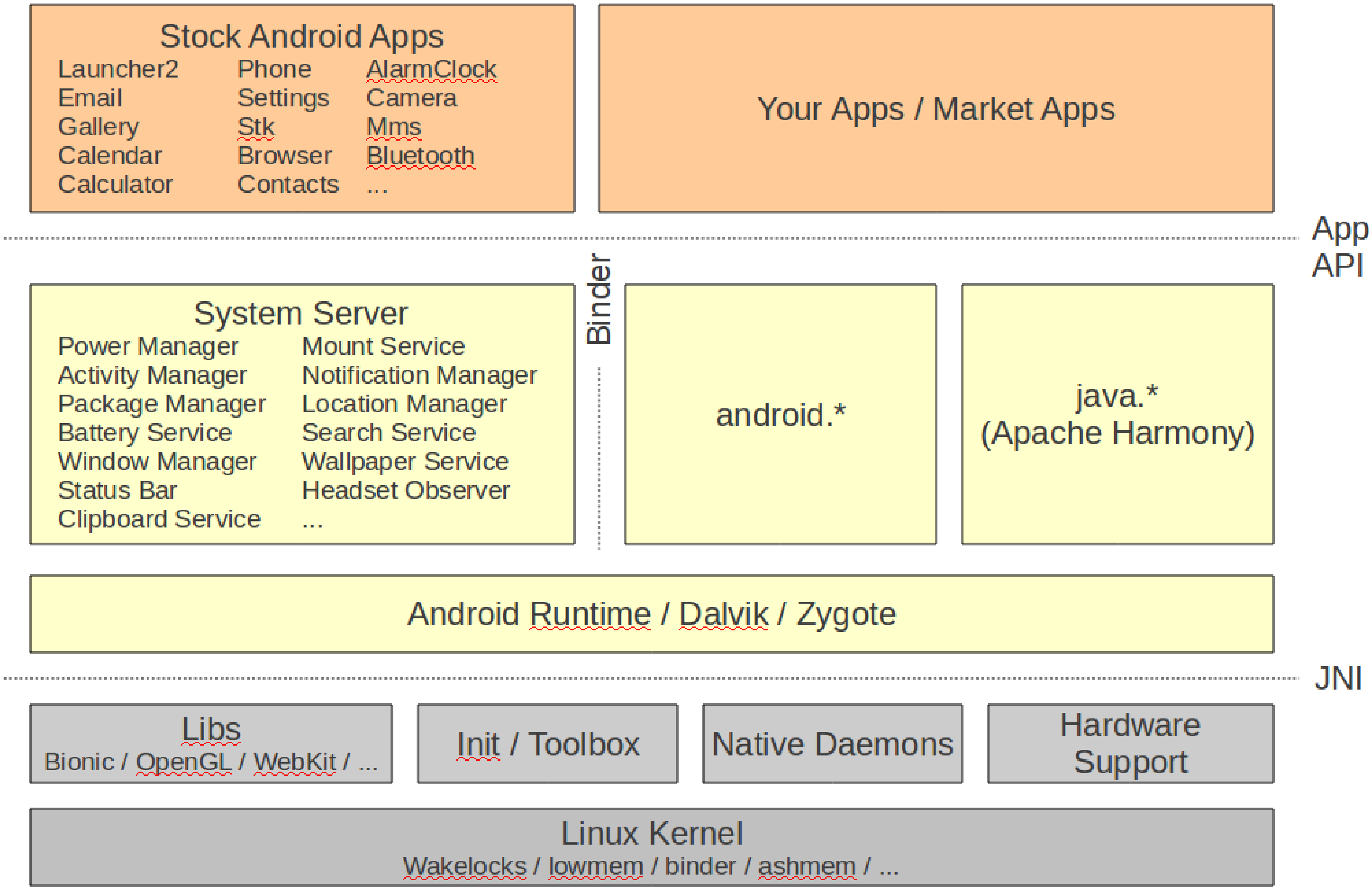
Android Montreal – November 3rd 2010

Karim Yaghmour / @karimyaghmour

>OPERSYS™

- Overall Architecture
- System startup
- Linux Kernel
- Hardware Support
- Native User-Space
- Dalvik
- JNI
- System Server
- Activity Manager
- Binder
- Stock Android Apps
- Hacking

Overall Architecture



Stock Android Apps

Launcher2 Phone AlarmClock
Email Settings Camera
Gallery Stk Mms
Calendar Browser Bluetooth
Calculator Contacts ...

Your Apps / Market Apps

App API

System Server

Power Manager Mount Service
Activity Manager Notification Manager
Package Manager Location Manager
Battery Service Search Service
Window Manager Wallpaper Service
Status Bar Headset Observer
Clipboard Service ...

Binder

android.*

java.*
(Apache Harmony)

Android Runtime / Dalvik / Zygote

JNI

Libs
Bionic / OpenGL / WebKit / ...

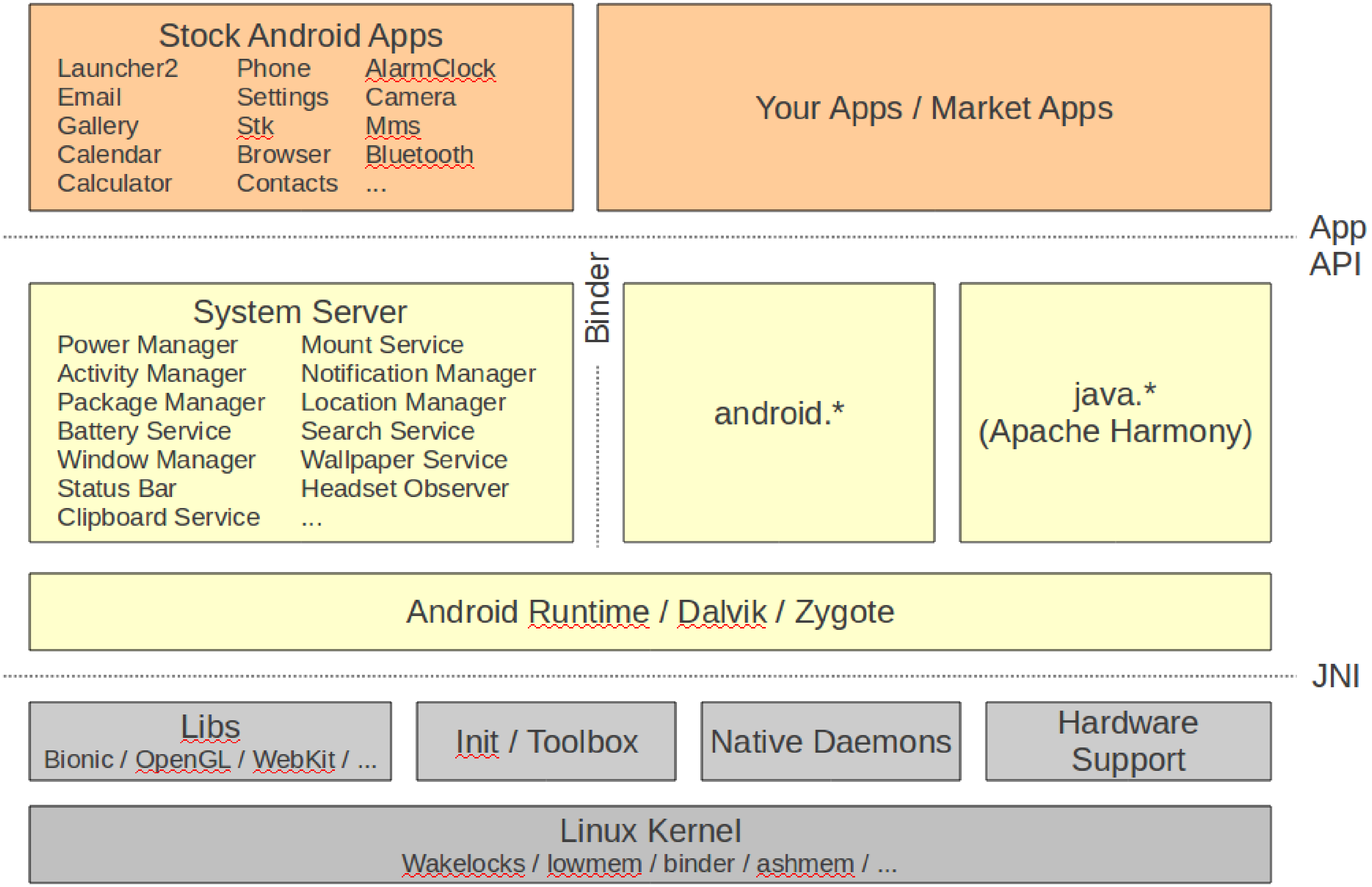
Init / Toolbox

Native Daemons

Hardware Support

Linux Kernel
Wakelocks / lowmem / binder / ashmem / ...

Arch vs. Tools



Stock Android Apps

Launcher2, Email, Gallery, Calendar, Calculator, Phone, Settings, Stk, Browser, Contacts, AlarmClock, Camera, Mms, Bluetooth, ...

Your Apps / Market Apps

App API

Binder

System Server

Power Manager, Activity Manager, Package Manager, Battery Service, Window Manager, Status Bar, Clipboard Service, Mount Service, Notification Manager, Location Manager, Search Service, Wallpaper Service, Headset Observer, ...

android.*

java.* (Apache Harmony)

Android Runtime / Dalvik / Zygote

JNI

Libs

Bionic / OpenGL / WebKit / ...

Init / Toolbox

Native Daemons

Hardware Support

Linux Kernel

Wakelocks / lowmem / binder / ashmem / ...

SDK, Eclipse, .apk

Manifest:
 Perms / SDK ver.

.dex, ddms

NDK, rootfs, initrc, adb

GNU toolchain

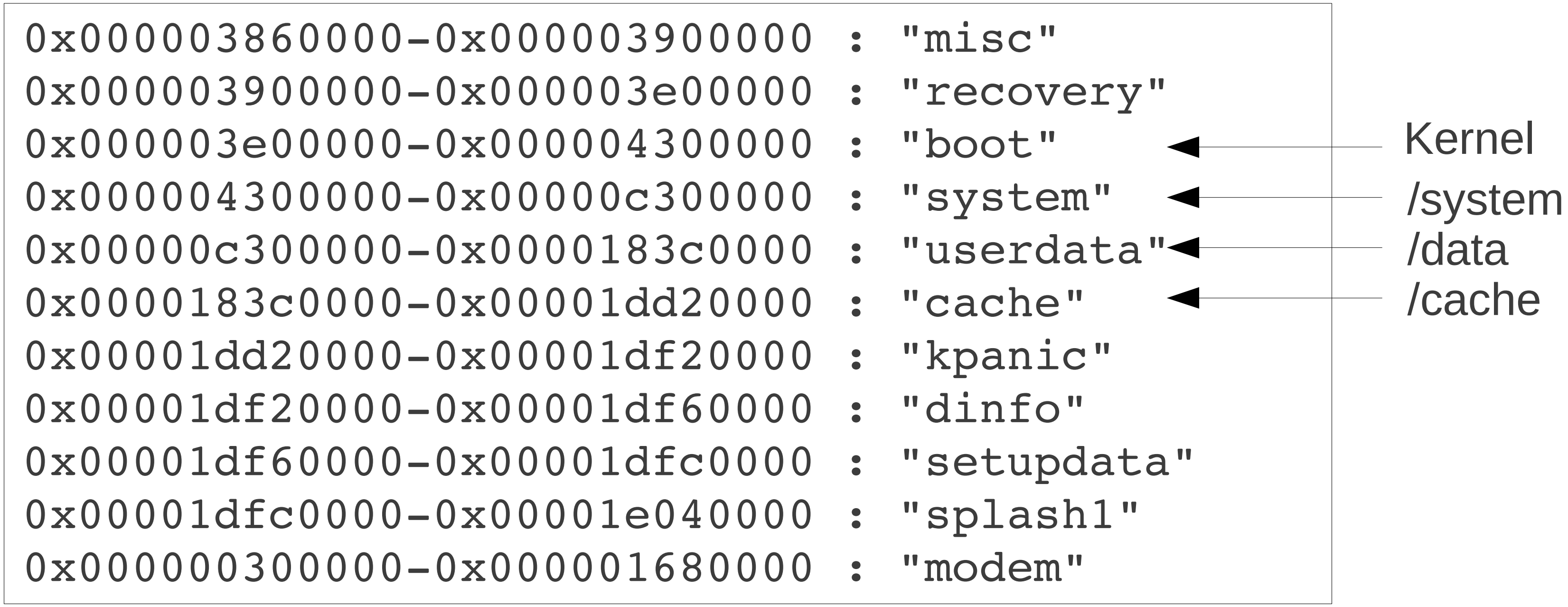
(fastboot)

System Startup

- Bootloader
- Kernel
- Init
- Zygote
- System Server
- Activity Manager
- Launcher (Home)

Startup - Bootloader

- CPU fetches first instruction from bootloader
- Bootloader boots kernel from flash:



```
0x000003860000-0x000003900000 : "misc"
0x000003900000-0x000003e00000 : "recovery"
0x000003e00000-0x000004300000 : "boot"
0x000004300000-0x00000c300000 : "system"
0x00000c300000-0x0000183c0000 : "userdata"
0x0000183c0000-0x00001dd20000 : "cache"
0x00001dd20000-0x00001df20000 : "kpanic"
0x00001df20000-0x00001df60000 : "dinfo"
0x00001df60000-0x00001dfc0000 : "setupdata"
0x00001dfc0000-0x00001e040000 : "splash1"
0x000000300000-0x000001680000 : "modem"
```

From Acer Liquid-E

Startup - Kernel

- Core kernel initialization
- Device drivers initialization
- Root filesystem mounting
- Execution of “/init”

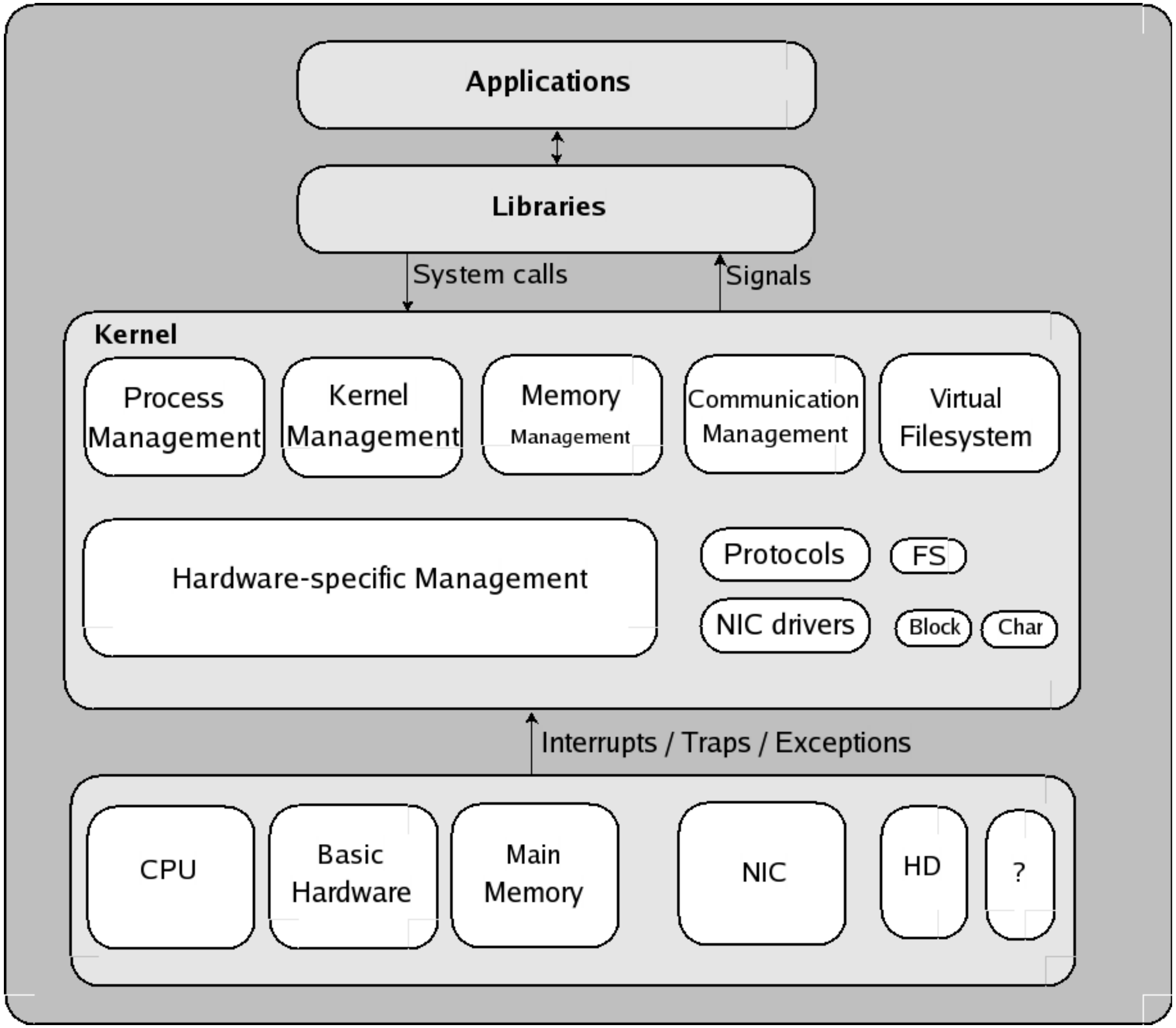
Startup - Init

- Open, parses, and runs /init.rc:
  - Create mountpoints and mount filesystems
  - Set up filesystem permissions
  - Set OOM adjustments properties
  - Start daemons:
    - adbd
    - servicemanager (binder)
    - vold
    - netd
    - rild
    - app_process -Xzygote (Zygote)
    - mediaserver
    - ...

Startup – Zygote, etc.

- app_main:
  - runtime.start(“com.android.internal.os.Zygote”, ...)
    - startVM()
    - Call Zygote's main()
      - preloadClasses()
      - startSystemServer()
      - ... magic ...
      - Call SystemServer's run()
        - Start **all** system services/managers
        - Start ActivityManager:
          - Send Intent.CATEGORY_HOME
            - Launcher2 kicks in

Linux Kernel – Generic Features



Linux Kernel - Androidisms

- Wakelocks
- lowmem handler
- Binder
- RAM console
- Logger
- ...

Hardware Support

Bluetooth	BlueZ through D-BUS IPC (to avoid GPL contamination it seems)
GPS	Manufacturer-provided libgps.so
Wifi	wpa_supplicant
Display	Std framebuffer driver (/dev/fb0)
Keymaps and Keyboards	Std input event (/dev/event0)
Lights	Manufacturer-provided liblights.so
Backlight	
Keyboard	
Buttons	
Battery	
Notifications	
Attention	
Audio	Manufacturer-provided libaudio.so (could use ALSA underneath ... at least as illustrate
Camera	Manufacturer-provided libcamera.so (could use V4L2 kernel driver underneath ... aga
Power Management	“Wakelocks” kernel patch
Sensors	Manufacturer-provided libsensors.so
Accelerometer	
Magnetic Field	
Orientation	
Gyroscope	
Light	
Pressure	
Temperature	
Proximity	
Radio Layer Interface	Manufacturer-provided libril-<companyname>-<RIL version>.so

Native User-Space

- Rootfs:
  - /system
  - /data
- Libs:

  Bionic, SQLite, SSL, OpenGL|ES,

  Non-Posix: limited Pthreads support, no SysV IPC
- Toolbox
- Daemons:

  vold, rild, netd, adbd, ...

Dalvik

- Sun-Java =

  Java language + JVM + JDK libs
- Android Java =

  Java language + Dalvik + Apache Harmony
- Target:
  - Slow CPU
  - Relatively low RAM
  - OS without swap space
  - Battery powered
- Now has JIT

Dalvik's .dex files

- JVM munches on “.class” files
- Dalvik munches on “.dex” files
- .dex file = .class files post-processed by “dx” utility
- Uncompressed .dex = 0.5 * Uncompressed .jar

JNI – Java Native Interface

- Call gate for other languages, such as C, C++
- Equivalent to .NET's pinvoke
- Usage: include and call native code from App
- Tools = NDK ... samples included
- Check out *“JNI Programmer's Guide and Specification”* - freely available PDF

System Server

Entropy Service
Power Manager
Activity Manager
Telephone Registry
Package Manager
Account Manager
Content Manager
System Content Providers
Battery Service
Lights Service
Vibrator Service
Alarm Manager
Init Watchdog
Sensor Service
Window Manager
Bluetooth Service

Device Policy
Status Bar
Clipboard Service
Input Method Service
NetStat Service
NetworkManagement Service
Connectivity Service
Throttle Service
Accessibility Manager
Mount Service
Notification Manager
Device Storage Monitor
Location Manager
Search Service
DropBox Service
Wallpaper Service

Audio Service
Headset Observer
Dock Observer
UI Mode Manager Service
Backup Service
AppWidget Service
Recognition Service
Status Bar Icons
DiskStats Service
ADB Settings Observer

Activity Manager

- Start new Activities, Services
- Fetch Content Providers
- Intent broadcasting
- OOM adj. maintenance
- Application Not Responding
- Ex. starting new app from Launcher:

  onClick(Launcher)->startActivity(Activity.java)->*Binder*->ActivityManagerService->startViaZygote(Process.java)->*Socket*->Zygote

Binder

- CORBA/COM-like IPC
- Data sent through “parcels” in “transactions”
- Kernel-supported mechanism
- Check /proc/binder/*

Stock Android Apps – from AOSP

/packages/apps

AccountsAndSettings
AlarmClock
Bluetooth
Browser
Calculator
Calendar
Camera
CertInstaller
Contacts
DeskClock
Email
Gallery
HTMLViewer
Launcher2
Mms
Music
PackageInstaller
Protips
Provision
QuickSearchBox
Settings
SoundRecorder
SpeechRecorder
Stk
VoiceDialer

/packages/providers

ApplicationProvider
CalendarProvider
ContactsProvider
DownloadProvider
DrmProvider
GoogleContactsProvider
MediaProvider
TelephonyProvider
UserDictionaryProvider

/packages/inputmethods

LatinIME
OpenWnn
PinyinIME

Hacking

- Source:
  - AOSP -- source.android.com / android.git.kernel.org
  - Cyanogenmod -- www.cyanogenmod.com
  - Moders sites ... aplenty ...
- Tools:
  - repo / git
  - fastboot
  - recovery
  - Kernel privilege escalation exploits -- “one-click root”
  - ...

AOSP contents

bionic	C library replacement
bootable	Reference bootloader
build	Build system
cts	Compatibility Test Suite
dalvik	Dalvik VM
development	Development tools
device	Device-specific files and components
external	Copy of external projects used by AOSP
frameworks	System services, android.*, Android-related cmds, etc.
hardware	Hardware support libs
libcore	Apache Harmony
ndk	The NDK
packages	Stock Android apps, providers, etc.
prebuilt	Prebuilt binaries
sdk	The SDK
system	pieces of the world that are the core of the embedded linux platform at the heart of Android.

Thank you ...

karim.yaghmour@opersys.com

>OPERSYS ™