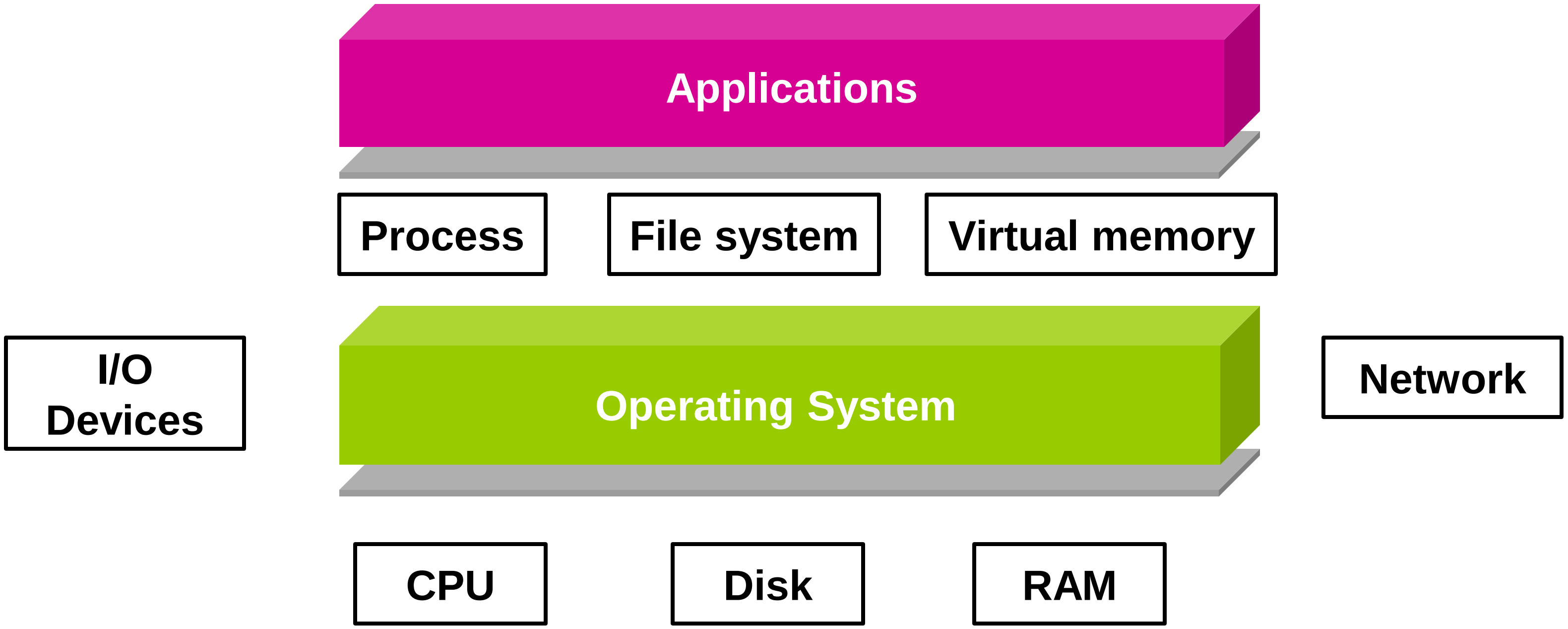
CS 153
Design of Operating Systems

Winter 2016

Lecture 24: Android OS

OS Abstractions



Applications

Process

File system

Virtual memory

I/O Devices

Operating System

Network

CPU

Disk

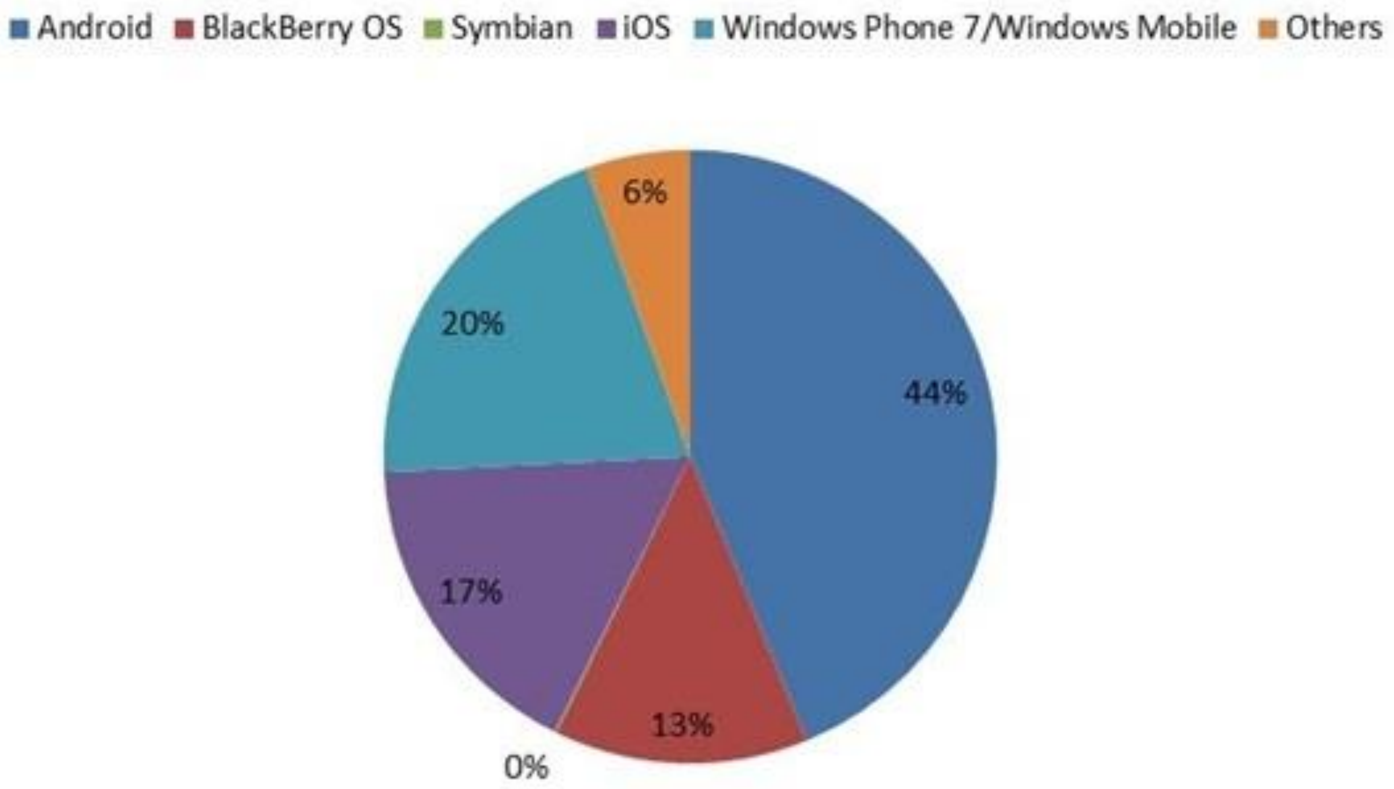
RAM

Smartphones

==

...in 2015

2015 Market Share*



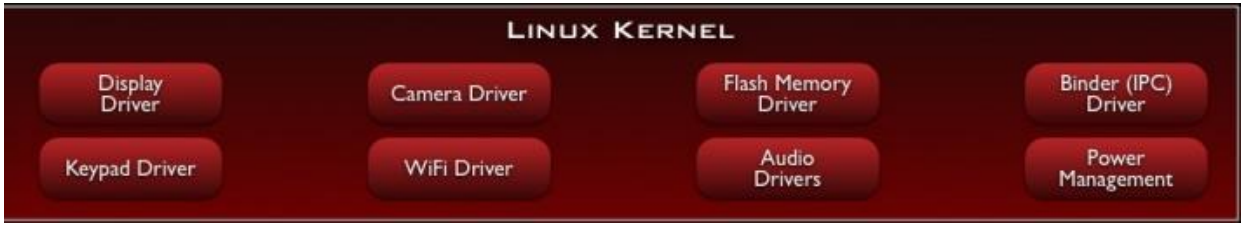
* Data provided by IDC Worldwide

What is the difference between a mobile OS and a desktop/server OS?

Differences

- Size / form-factor
  - UI system design?
- Resource-constrained (e.g., battery, memory)
  - Optimized OS (what would you do?)
- Cellular and other hardware components
- User has no root access
  - Unless OS has vulnerabilities and get compromised
- Security threats
  - App is fully sandboxed and cannot easily attack other apps

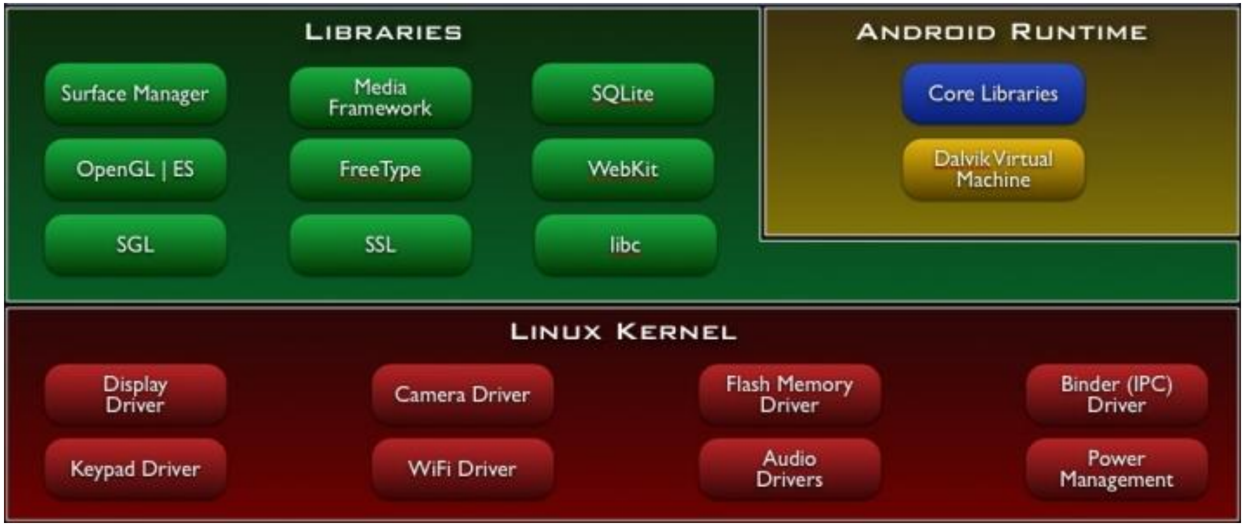
Android


LINUX KERNEL
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

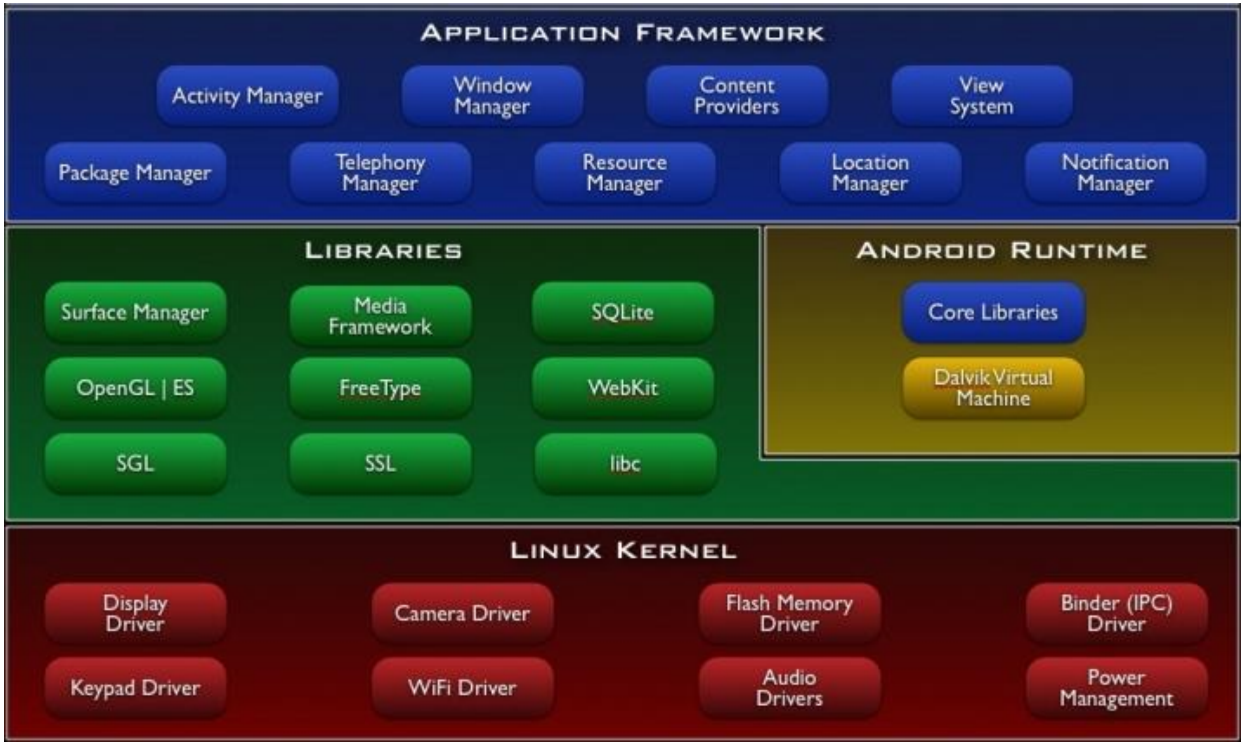
Based on Linux

- Linux on ARM
- Drivers and architecture support
  - How to port Android to a new device?
- Using Linux vs. Writing a new OS from scratch?
  - Do all Linux kernel implementations work well on mobile devices?

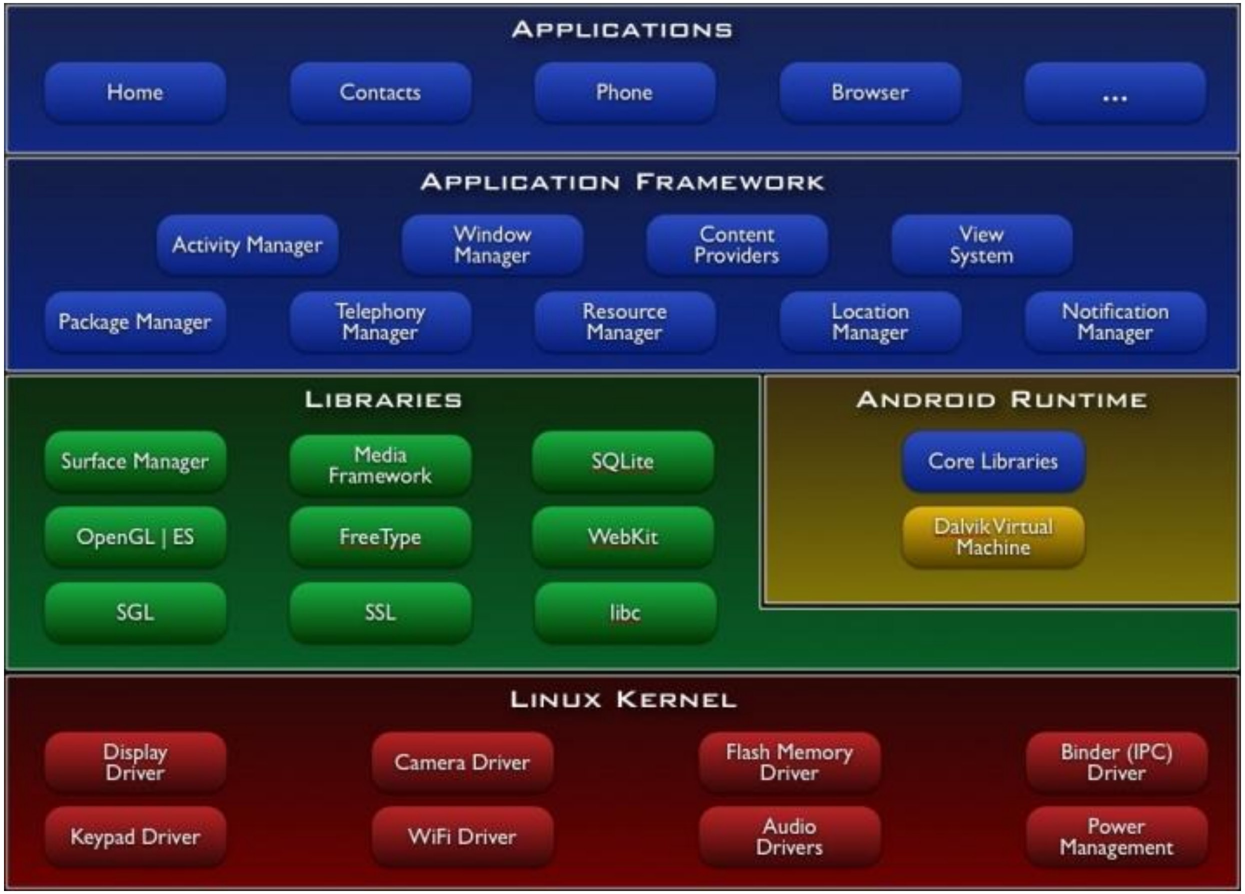
Android


Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
Android Runtime
Core Libraries
Dalvik Virtual Machine
Linux Kernel
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Android


APPLICATION FRAMEWORK
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
LIBRARIES
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine
LINUX KERNEL
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Android


Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
Android Runtime
Core Libraries
Dalvik Virtual Machine
Linux Kernel
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Differences

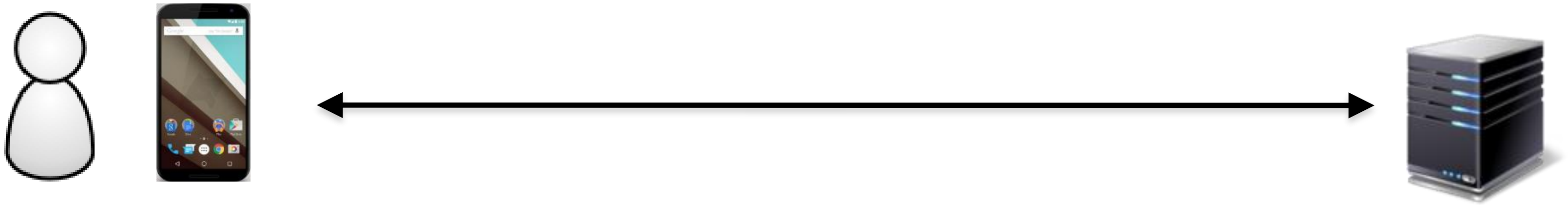
- Size / form-factor
- Resource-constrained (e.g., battery, memory)
  - Optimized OS (what would you do?)
- Cellular and other hardware components
- User has no root access
  - Unless OS has vulnerabilities
- Security threats
  - Malware is fully sandboxed and cannot easily attack other apps

Resource-constrained devices

- How would you optimize the OS in the following aspects?
  - Scheduling
    - Hint: priority
  - Memory management
    - Hint: memory pressure
  - File systems
    - Hint: access control
  - Others?

Offloading of Computation

- Naive offloading
  - Speech-to-text, OCR, Apple’s Siri
- More sophisticated offloading - fine-grained offloading
  - MAUI: Making Smartphones Last Longer with Code Offload
  - Running two versions of the app on the mobile device and a powerful server
  - Decide when/what to offload on the fly



Differences

- Size / form-factor
- Resource-constrained (e.g., battery, memory)
  - Optimized OS (what would you do?)
- Cellular and other hardware components
- User has no root access
  - Unless OS has vulnerabilities
- Security threats
  - Malware is fully sandboxed and cannot easily attack other apps

Disk I/O

	Flash	Hard Disk Drive
Random access	~0.1ms	5-10ms
File fragment impact	No	Greatly impacted
Total power	1/2 to 1/3 of HDD	up to 15+ watts
Reliability	Reliable	Less reliable due to mechanical parts
Write longevity	Limited number of writes	Less of a problem
Capacity	<= 1TB	4TB
Price	$0.4 / GB	$0.04 / GB

New Capabilities

- Cellular
  - Make phone calls
  - Send/Recv SMS
- GPS
  - Tracking
- Phone number
  - Identification
- Application data
  - Bank account info

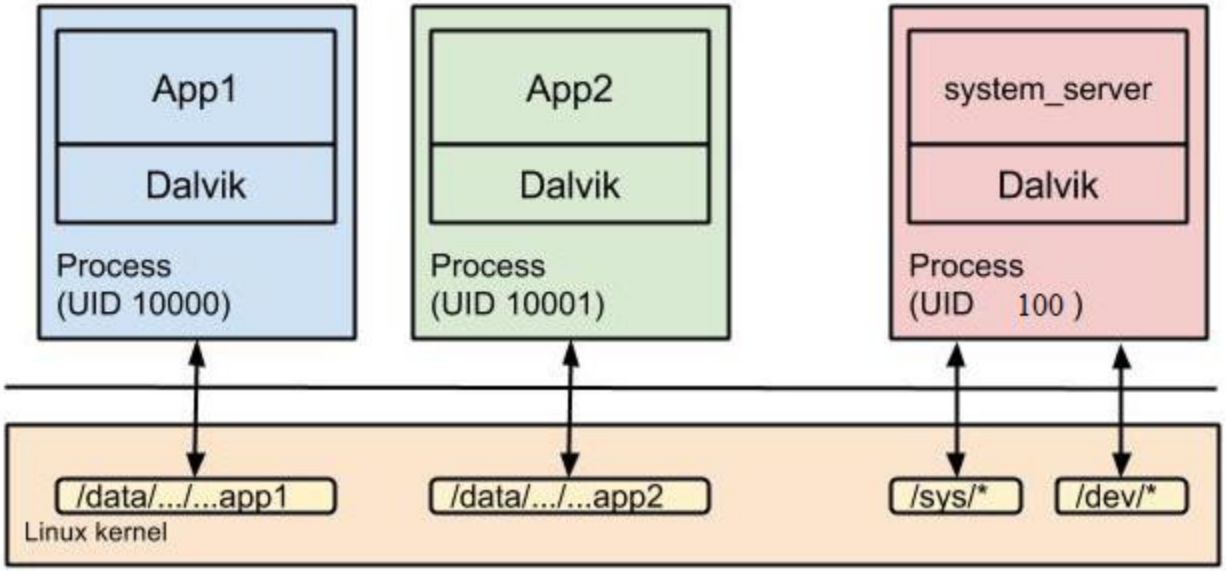
…

- How to secure them?

Android Security

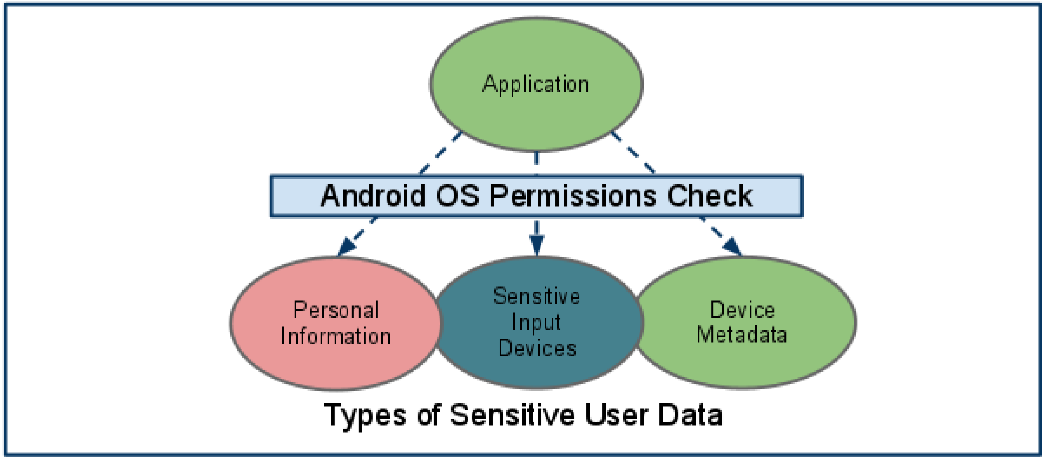
Android Sandbox

- UID separation to protect apps from each other

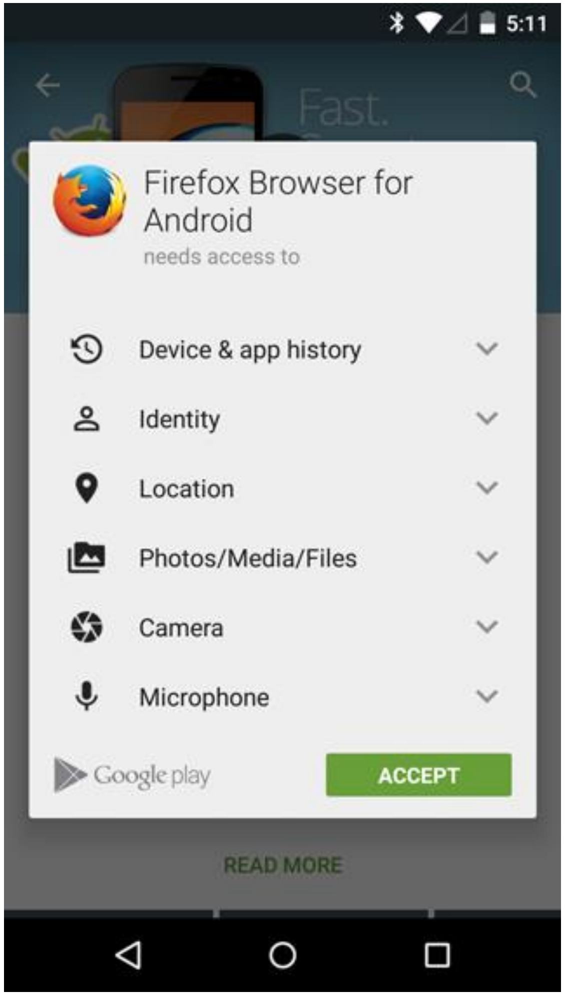


Android Permission

- Apps need permissions when they attempt to
  - access sensitive resource *or*
  - perform sensitive operations



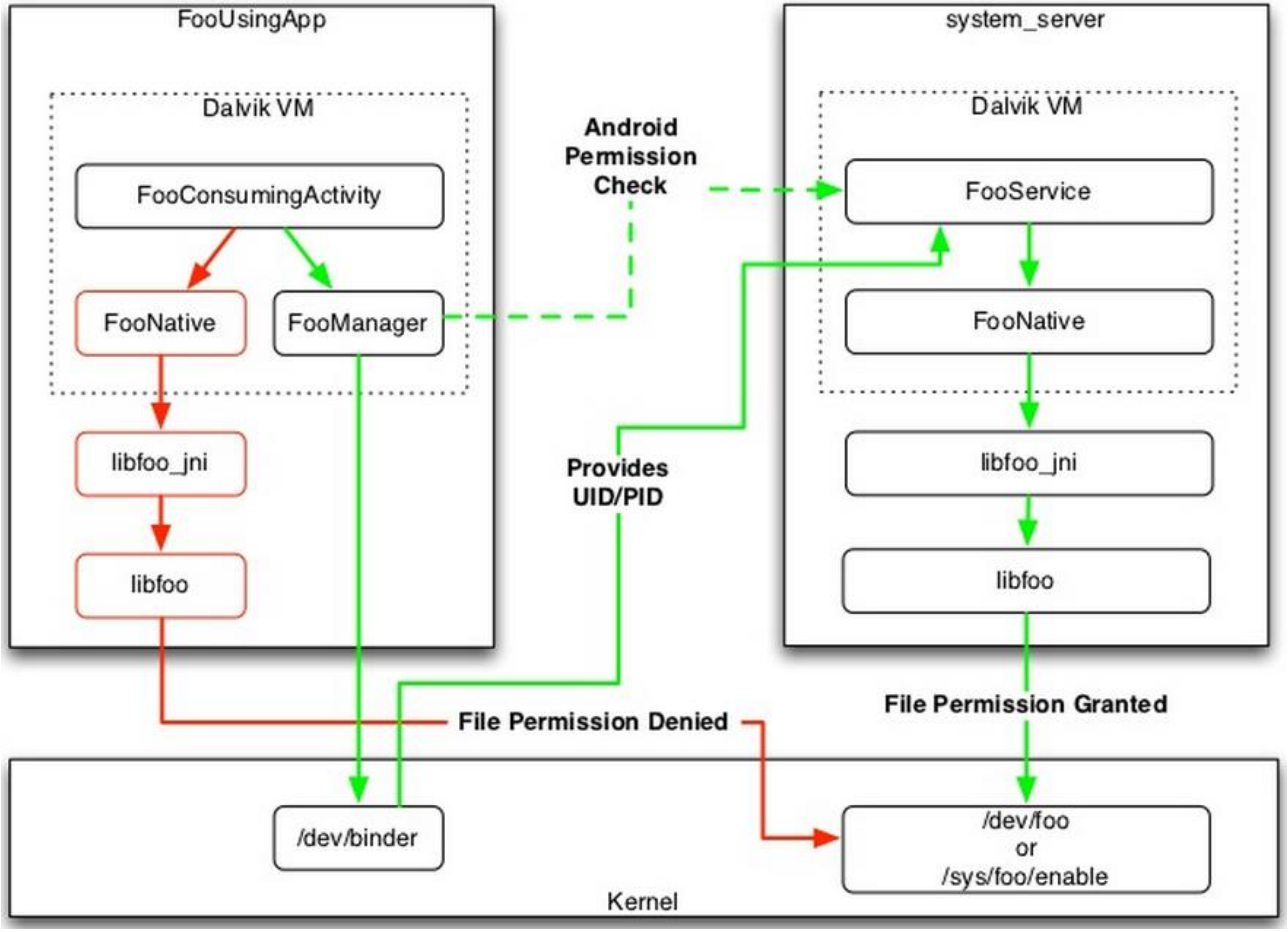
Types of Sensitive User Data



Firefox Browser for Android
needs access to

- Device & app history
- Identity
- Location
- Photos/Media/Files
- Camera
- Microphone

Permission enforcement



Permission enforcement (gid)

- Enforced in kernel through uid

- Kernel code in net/ipv4/af_inet.c:

```
#include <linux/android_aid.h>
static inline int current_has_network(void) {
    return in_egroup_p(AID_INET) ||
                          capable(CAP_NET_RAW);
}
```

Differences

- Size / form-factor
- Resource-constrained (e.g., battery, memory)
  - Optimized OS (what would you do?)
- Cellular and other hardware components
- User has no root access
  - Unless OS has vulnerabilities
- Security threats
  - Malware is fully sandboxed and cannot easily attack other apps

Android Root

- No app can run with root privilege in Android
  - even if the user desires
- Restrictions set by Google, Vendors, and Carriers
  - Result: bloatware, power inefficiency, lost freedom/functionality, etc.
- How do we gain root back?

Background: Symbolic Link

- On most file systems, symbolic link is supported to point to the same file content without having to copy the content

- “ln –s /home/zhiyunq/ /shortcut”
- /shortcut → /home/zhiyunq

File Permission Vulnerabilities

- Works on certain Android devices
  - Customized by vendors such as Motorola or Samsung

- Goal: Write to /data/local.prop
  - Add line ro.kernel.**qemu**=**1**
  - But permission denied to normal app

- Exploit:
  - rm /data/local/logs/log.txt (accessible to anyone)
  - ln -s /data/local.prop /data/local/logs/log.txt
  - What is the vulnerability?

Summary

- Android OS vs. Traditional OS
- Security architecture of Android
- Android root exploit through file permission vulnerability