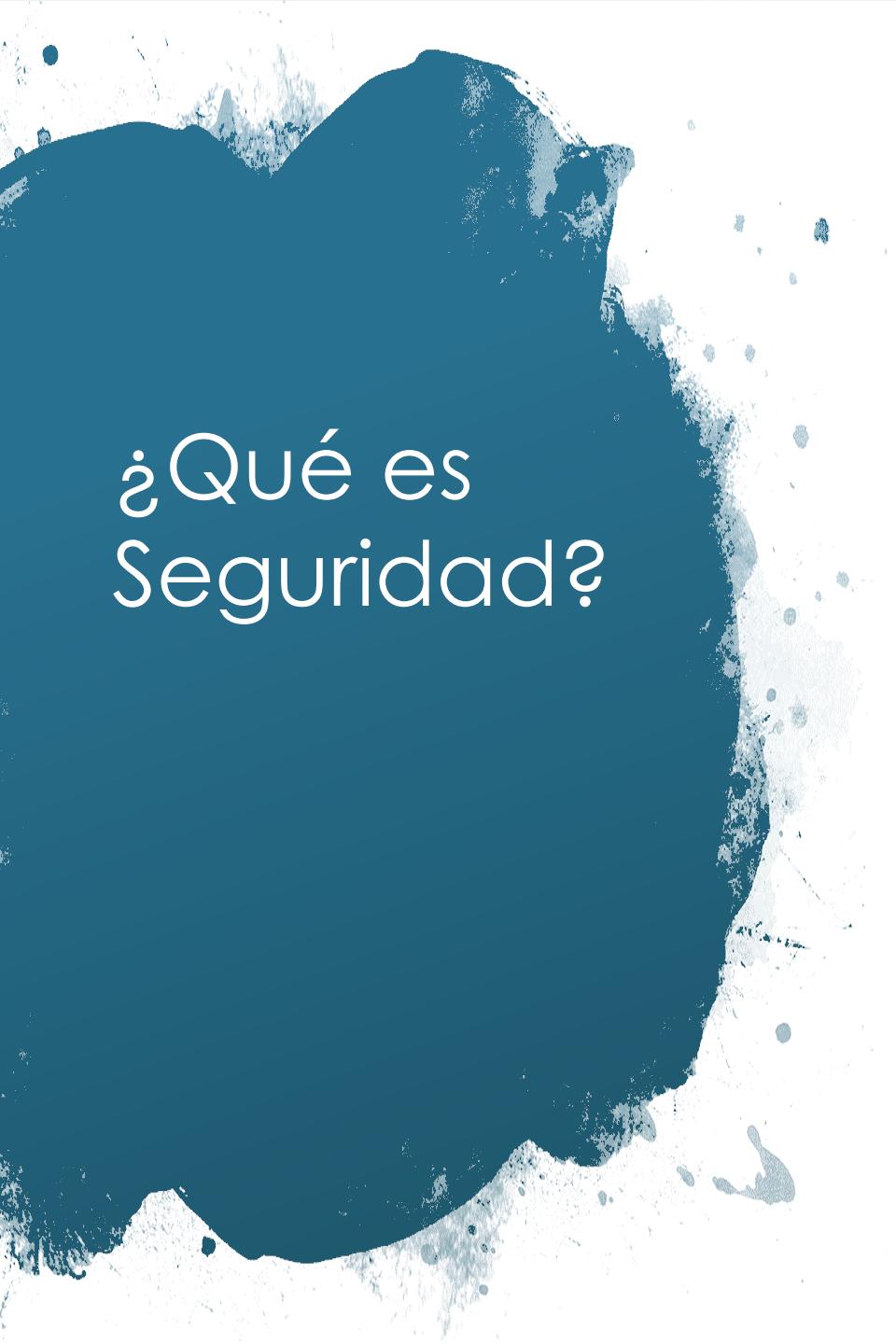




# Seguridad

Ingenieria de Software en la Practica



# ¿Qué es Seguridad?

- No tiene demasiado sentido hasta que definamos qué es estar seguro y seguros de qué/quien.
- De la misma manera, la seguridad es difícil de entender sin una amenaza potencial

# Diferenciales Móviles



Modelo  
diferente a  
PC o  
Servidores

único  
Infor  
maci  
ón  
con  
alto  
valor  
Aplic  
acio  
nes  
de



Disponibilidad



Resistencia a  
ataques locales

# Diferenciales móviles

---



**La seguridad física no existe**



**Los teléfonos se pierden!**



**Se necesitan formas de proteger los datos**

Encriptación local

Almacenamiento en la nube

# Limitantes



Ancho de banda



Energía



CPU

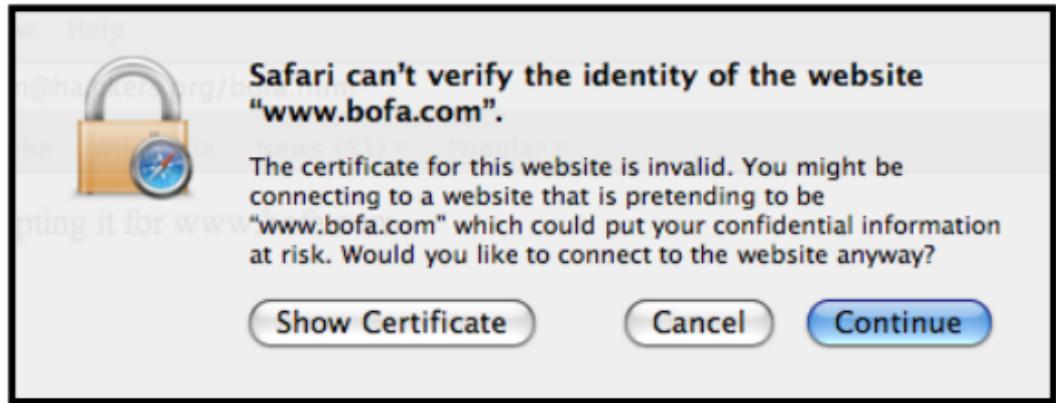


Tamaño



Eventualmente el avance de la tecnología va a remover estas limitantes, pero ... el problema lo tenemos ahora!

# Ejemplo de limitante: Pantalla





Otro ejemplo:  
teclado

C)sOz\*ao1pdn

## Otro ejemplo: Regulaciones



# Amenazas

- Divididas por actores. Todos “usan” los dispositivos y tienen diferentes objetivos:
  - Sistema Operativo (Fabricantes): modelo de seguridad.
  - Usuarios: software malicioso, troyanos, mecanismos débiles de seguridad.
  - Operadores de red: mecanismos de identificación telefónica, software de red, problemas en mecanismos de SIM
  - Proveedores de Contenido: quieren obtener beneficios.
    - Problemas con mecanismos de DRM, etc.

## Proveedores de contenido y aplicaciones

Derechos de autor y pago por el uso de las apps.

Relación indirecta con el usuario final.

Dificultades de actualización

Alto desfasaje de tiempo para la actualización

Múltiples plataformas de hardware

# Sistemas operativos

- Seguridad en lenguajes de programación
- Herencia de escritorio



# Usuarios



Seguridad en el manejo de la información



Confiabilidad en el intercambio de información (ej. Transacciones comerciales)



Confidencialidad de los datos.

# Cómo medimos la Seguridad?

- La seguridad puede medirse sobre cuatro ejes básicos:
  - Confidencialidad (criptografía de datos)
  - Integridad (asegurar que la información no haya sido modificada o adulterada)
  - Autenticación (proceso por el cual una unidad garantiza con otra ser quien dice ser)
  - Autorización (dar acceso a cierta funcionalidad o información a una unidad autenticada)

# Objetivos de Seguridad



QUE LOS USUARIOS  
PUEDAN EJECUTAR  
APLICACIONES DE  
MANERA SEGURA



QUE EL SISTEMA  
OPERATIVO ESTÉ  
PROTEGIDO DE LAS  
APLICACIONES



DATOS PRIVADOS POR  
APLICACIÓN



EVITAR  
VULNERABILIDADES

# Taxonomía de problemas de seguridad



Autenticación y autorización segura de nodos



Comunicación segura entre nodos autorizados



Deployment seguro de aplicaciones sobre dispositivos



Almacenamiento y recuperación seguras de información sobre el dispositivo



Asegurar información provista por el dispositivo (como ser información de localización)

# Seguridad en Aplicaciones Móviles



La mayor parte de las aplicaciones móviles, son básicamente aplicaciones distribuidas.



La seguridad está íntimamente relacionada con la plataforma específica en la que se desarrolla

# Vulnerabilidades por OS

---

rank	browser	number of vulnerabilities
1	Apple iOS	375
2	Microsoft Windows RT 8.1	139
3	Microsoft Windows RT 8	138
4	Google Android	130
5	Apple Watch OS	53
6	Apple TV OS	46

# Dos Modelos

---

Old Way

Normal

Privileged

New Way

App

App

App

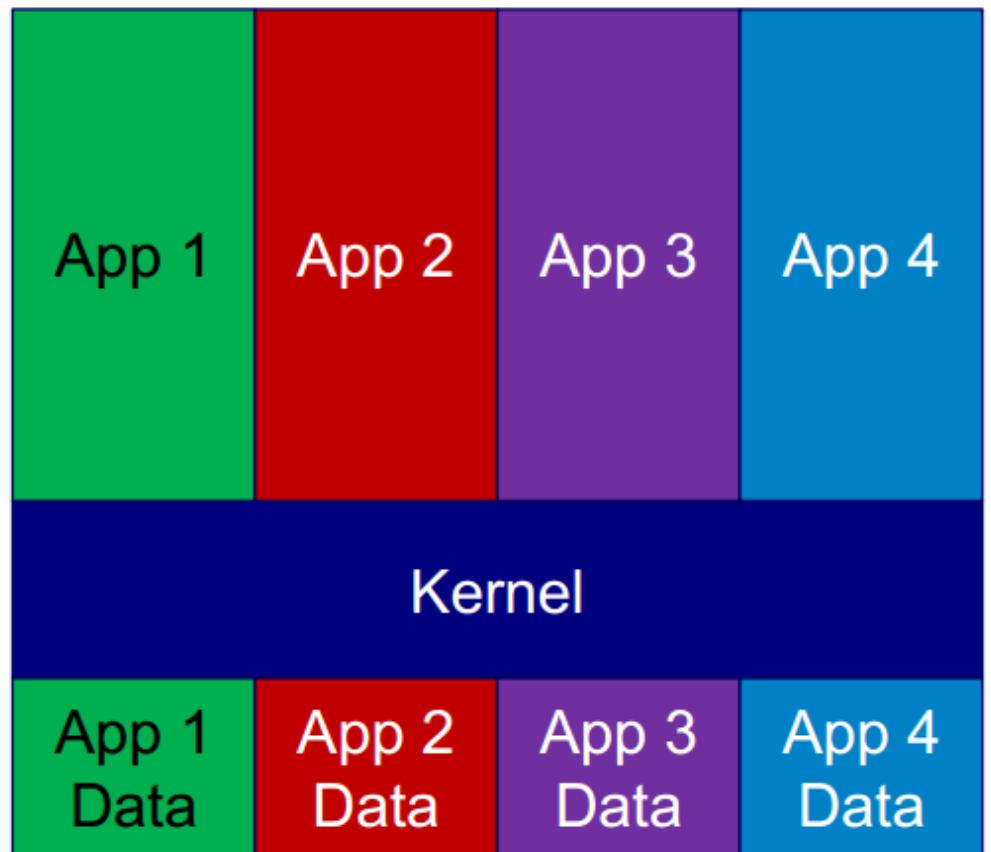
App

App

App

iOS

---



# iOS



Modelo de distribución único



Políticas estrictas para la AppStore



Políticas aplicadas por fuera de la tecnología



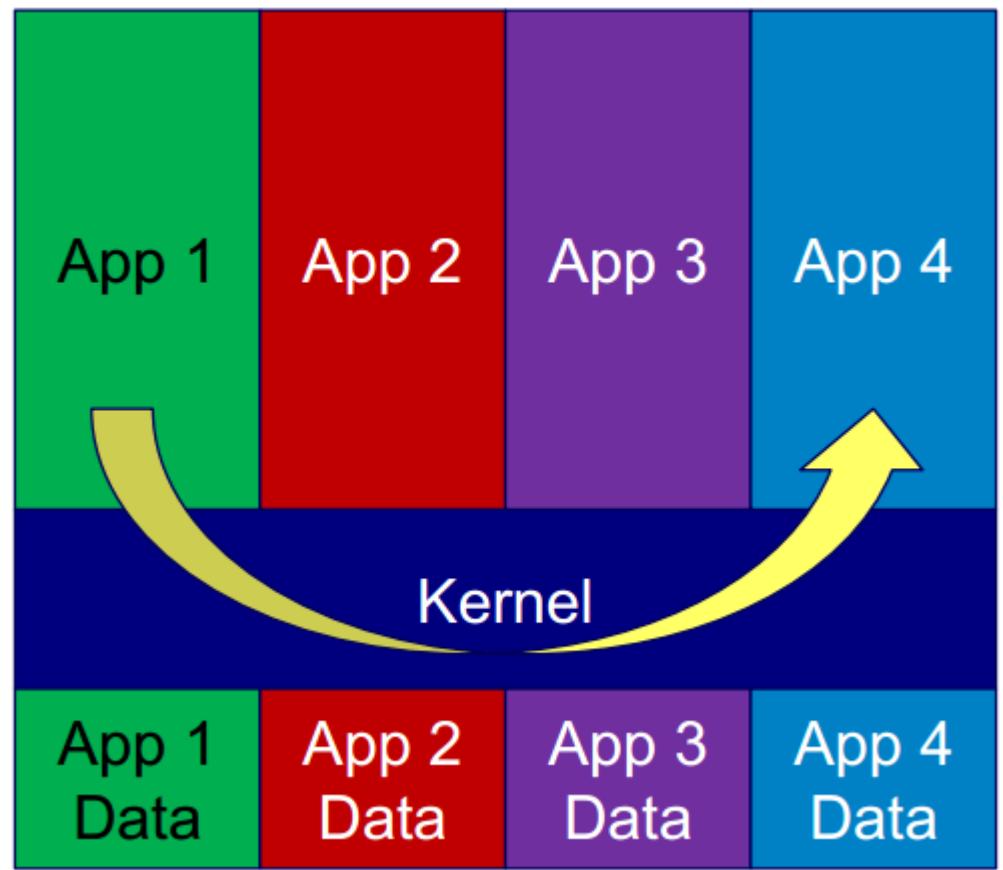
El AppStore es una barrera de Seguridad



Problemas con “Jailbreak”

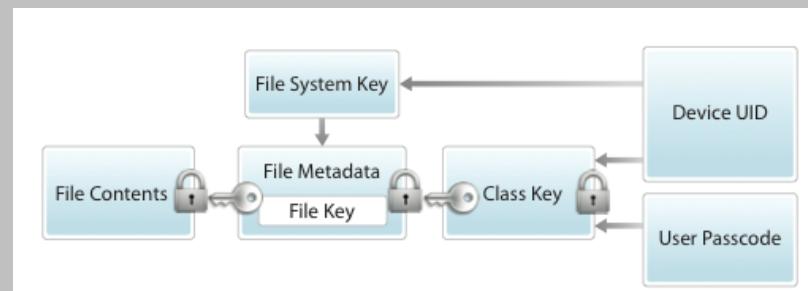
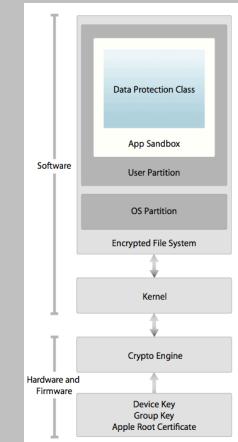
# Android

---



# Arquitectura Seguridad iOS

- Cadena segura de carga (boot)
- System Software Personalization (para actualizaciones de S.O. y apps)
- Firma digital de Aplicaciones
- Runtime Process Security
- Encripción de datos por Hardware
- File System Encriptado
- PassCodes
- Seguridad de Red (VPN, SSL, TLS, WiFi protocols)



# Data Protection Classes

- `NSFileProtectionComplete`  
(por ejemplo Mail)
- `NSFileProtectionCompleteUnlessOpen`
- `NSFileProtectionCompleteUntilFirstUserAuthentication`
- `NSFileProtectionNone`

# Problemas específicos de plataforma móvil

- Pérdida o robo de dispositivos. Mucho más probable perder un teléfono que un PC.
- Si bien tecnología para soluciones location-based pueden funcionar como paliativo para este problema. Al momento de encontrar el dispositivo, la información ya puede haberse visto comprometida

# Problemas específicos de plataforma móvil

- Múltiples ambientes de conectividad:
  - Con o sin VPN
  - Conectarse directamente a la red, o a través de un ISP corporativo, o personal

# Panorama Actual

- Symbian (casi desaparecido)
- Poca presencia en el mundo
- Fue el Sistema Operativo más atacado.
- 99% del malware estuvo enfocado en este S.O.
- Es inseguro? NO!  
Practicamente la única forma de ser infectado es evitar todas las alertas del S.O.

# Panorama Actual

- iPhone
  - Problemas principales generados con los dispositivos 'jailbroken' con aplicaciones no autorizadas
  - Problemas de diseño de la plataforma:
    - MobileSafari + MobileEmail
    - Todas las aplicaciones corren como root, si hay un bug, se pueden permitir permisos de acceso remoto al shell del teléfono (y comprometer privacidad, etc)
  - Esto solo es posible luego del jailbreaking
  - 40% de los dispositivos jailbroken ☺

# Panorama Actual

- Android:
  - Comienza a aparecer malware.
  - Problemas en Adobe Flash
  - Relativamente segura en comparación a Symbian pero alto crecimiento de ataques

# Seguridad en android

- Objetivos
  - Proteger la información del usuario
  - Proteger los recursos del sistema (incluyendo la red)
  - Proveer aislamiento para las aplicaciones

# Características Fundamentales



Seguridad robusta a nivel del sistema operativo (Linux Kernel)



Sandbox obligatorio para las aplicaciones



Comunicación inter procesos segura



Firmado de aplicaciones



Permisos definidos a nivel de aplicación y concedidos por el usuario.

# A nivel del Sistema Operativo

Modelo de permisos basado en los usuarios

Aislamiento de procesos

Mecanismo extensible para IPC

Permite eliminar partes innecesarias y potencialmente peligrosas del SO.

# Sandbox para aplicaciones



Android asigna un usuario a cada aplicación instalada.



Cada aplicación corre como un usuario distinto en un proceso distinto.



Las aplicaciones no pueden interactuar entre si ni afectar recursos de otra aplicación.



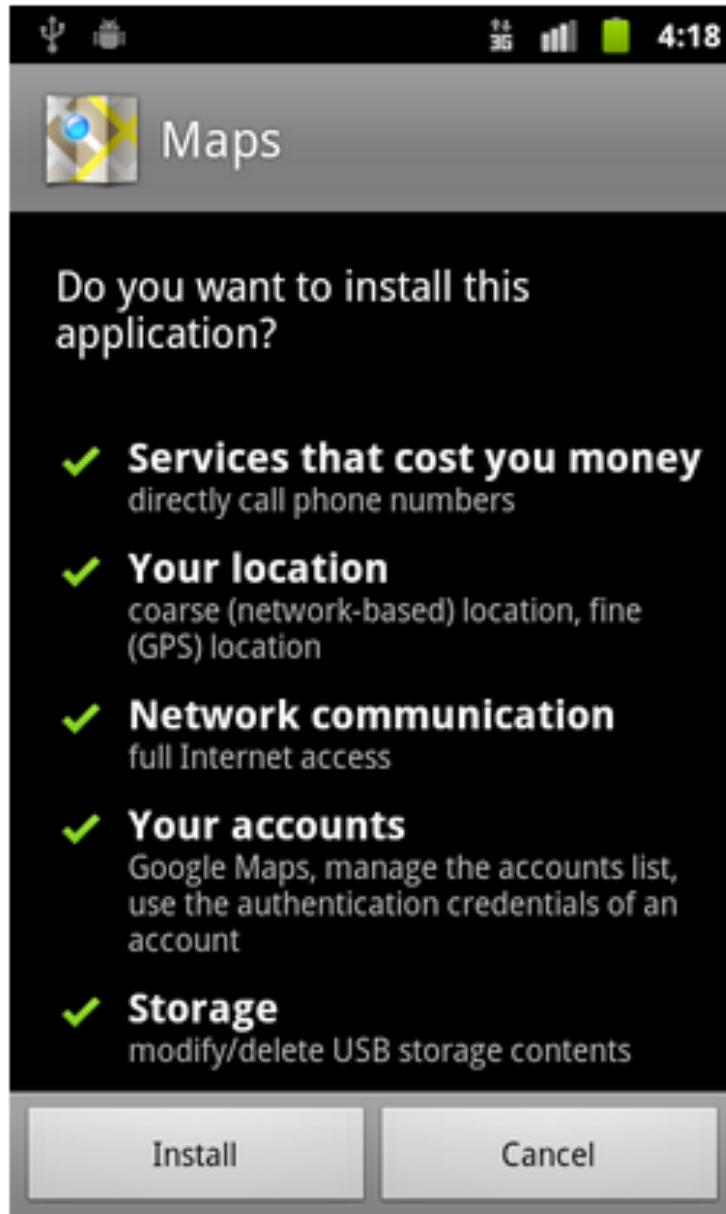
Sandbox a nivel del SO.

# El modelo de permisos

- Todos los recursos del dispositivo son accesibles mediante el sistema operativo.
- Para esto las aplicaciones deben declarar las capacidades que necesitan en su manifiesto.

# Decisión final del usuario

---



# Comunicación entre Procesos

- Binders y services
- Intents
- Content Providers

# Cost- Sensitive APIs

- Cualquier api que puede generar costos al usuario o la red.
- El usuario debe dar permiso específico a las aplicaciones que así lo requieran.
- Ejemplos
  - Telefonía
  - SMS / MMS
  - Network
  - InApp Billing

# Acceso a la SIM



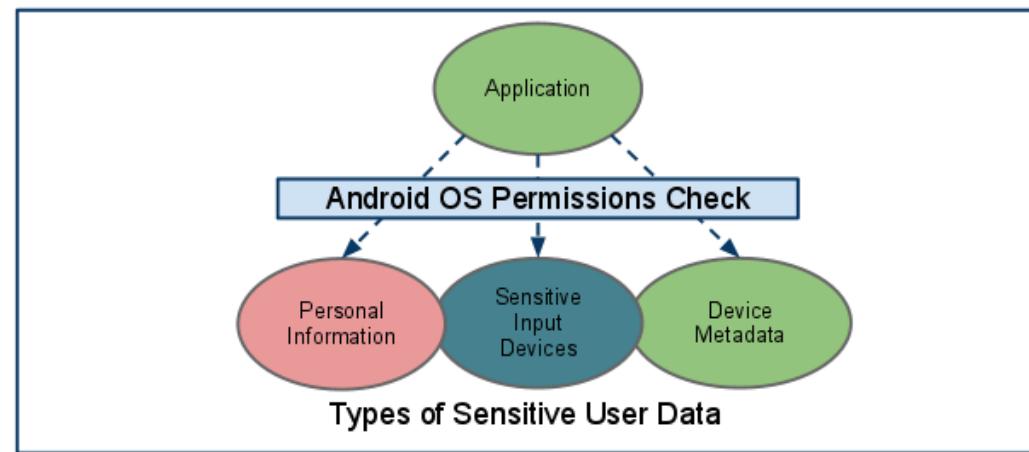
El acceso a bajo nivel a los datos de la SIM no está permitido para las aplicaciones de terceros.



El SO controla todos los accesos a la SIM incluyendo los contactos.

# Modelo de Permisos

---

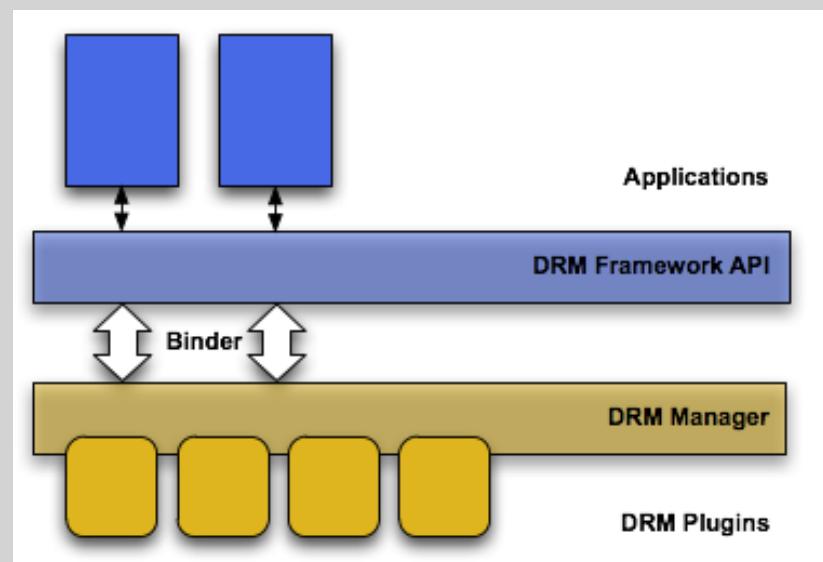


# Firma de aplicaciones

- Las aplicaciones deben estar firmadas digitalmente (Certificado digital) para poder ser publicadas en Google Play
- El instalador de paquetes de android por defecto no permite instalar aplicaciones que no estén firmadas (se puede deshabilitar en dispositivos para desarrollo)

# DRM

- Android provee un framework para DRM extensible que permite a las aplicaciones administrar contenido con derechos protegidos.



# Otros Recursos

- Guía de Seguridad para android

<http://source.android.com/devices/tech/security/>

Información de seguridad para desarrolladores:

<https://developer.android.com/training/articles/security-tips.html>