http://www.softwareinlife.com

Android Security

Jang, Sun-Jin

CEO of Software in Life Inc.

(@jangsunjin, jangsunjin@softwareinlife.com)

Software in Life

We Create Good Software for People.

Table of Contents

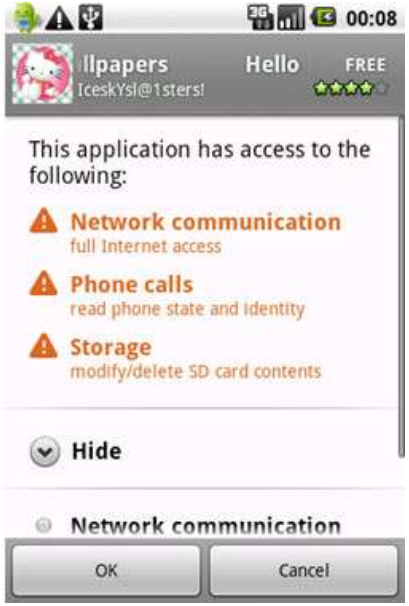
Software in Life

I. Mobile Security

1. Mobile Security Issues
2. Mobile Security Definition
3. Mobile Threats and Attacks
4. Smartphone Security
5. Smartphone Security Responsibilities
6. Smartphone Security Chain
7. Mobile Security Platform Needs

Steeling Information

Jackeey Wallpaper　　Eoeandroid Wallpaper

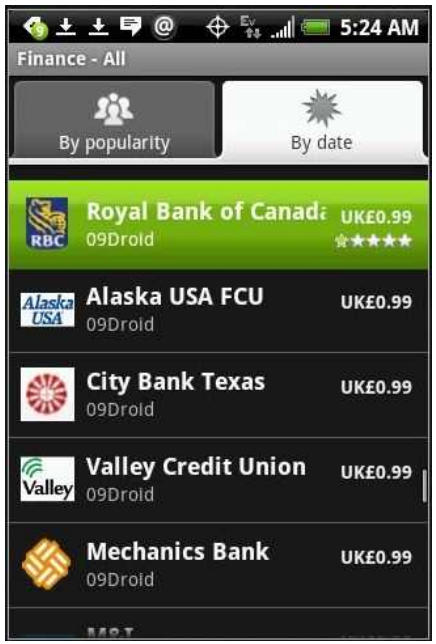


- 대표적인 개인정보유출 악성 앱은 미국에서 열린 '블랙햇 USA 2010'에서 지목돼 화두가 됐던 '재키 월페이퍼(Jackeey Wallpaper)'이다.

- 기존의 악성 앱은 국제모바일기기식별번호(IMEI) 와 휴대폰 정보만을 수집했던 반면에 최근 분석된 앱은 전화번호, IMEI, SIM 국가정보, SIM 시리얼 넘버, SIM IMSI, 보이스 메일 번호, 이메일, 인터넷 히스토리 정보, 문자정보, 네트워크 접속방법, 접속위치 등 대부분의 개인정보를 수집할 수 있다.

※ http://www.intomobile.com/2010/07/29/downloaded-jackeey-wallpaper-for-android-your-personal-information-is-now-on-some-chinese-server/

Phishing Banking Information

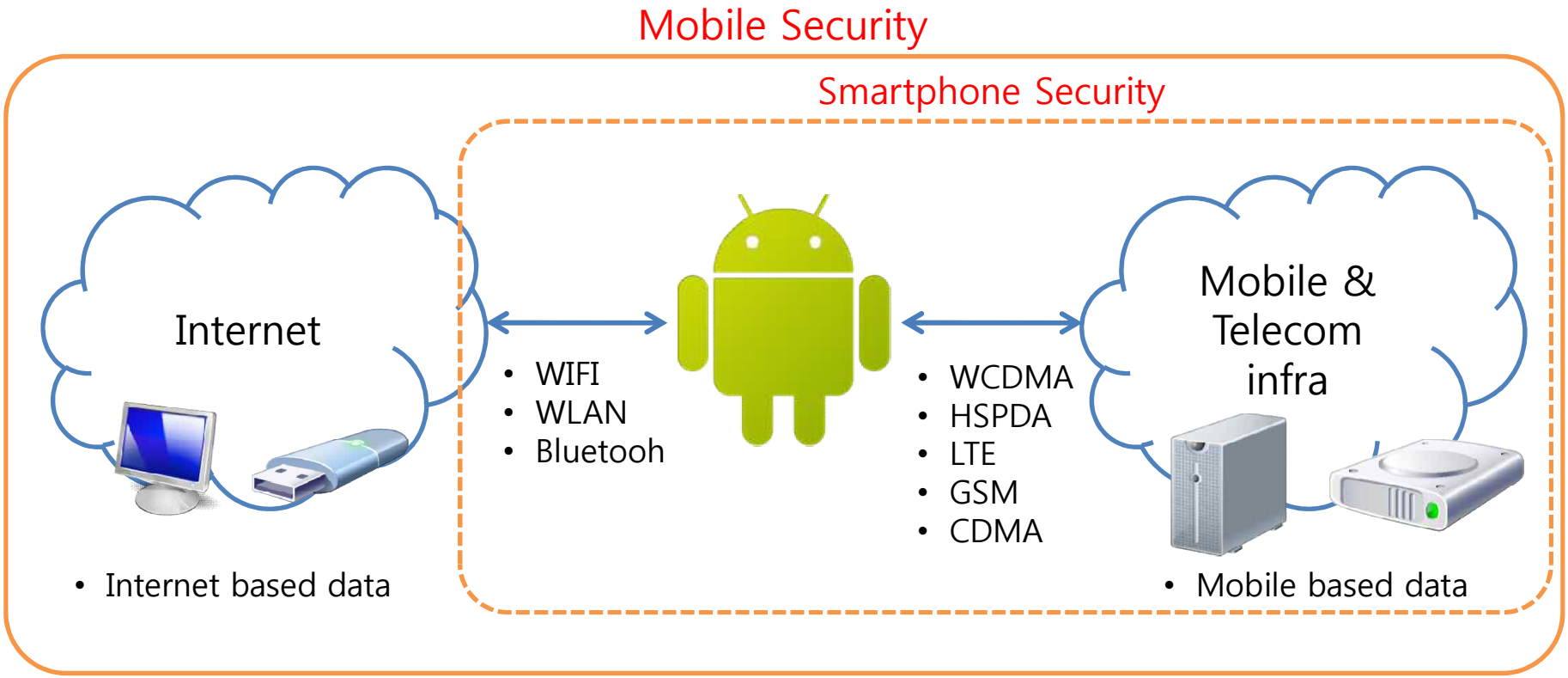


- 보안업체인 에프-시큐어(F-Secure)에 따르면, '드로이드09(Droid09)'라는 개발자가 인터넷 뱅킹 프로그램처럼 보이도록 만들어, 금융 기관명을 도용하여 안드로이드 마켓에서 판매하였다.
- Royal Bank of Canada 등의 프로그램은 미국은행을 비롯해 다수의 신용조합 이름을 프로그램 이름으로 사용하고 있어 이용자의 각별한 주의를 필요로 한다. 문제의 안드로이드 앱이 발견된 후 '드로이드09' 계정의 프로그램의 판매는 중지되었으며, 금융기관들도 자사 고객들에게 불법 프로그램에 대한 공지를 띄운 것으로 전해지고 있다.

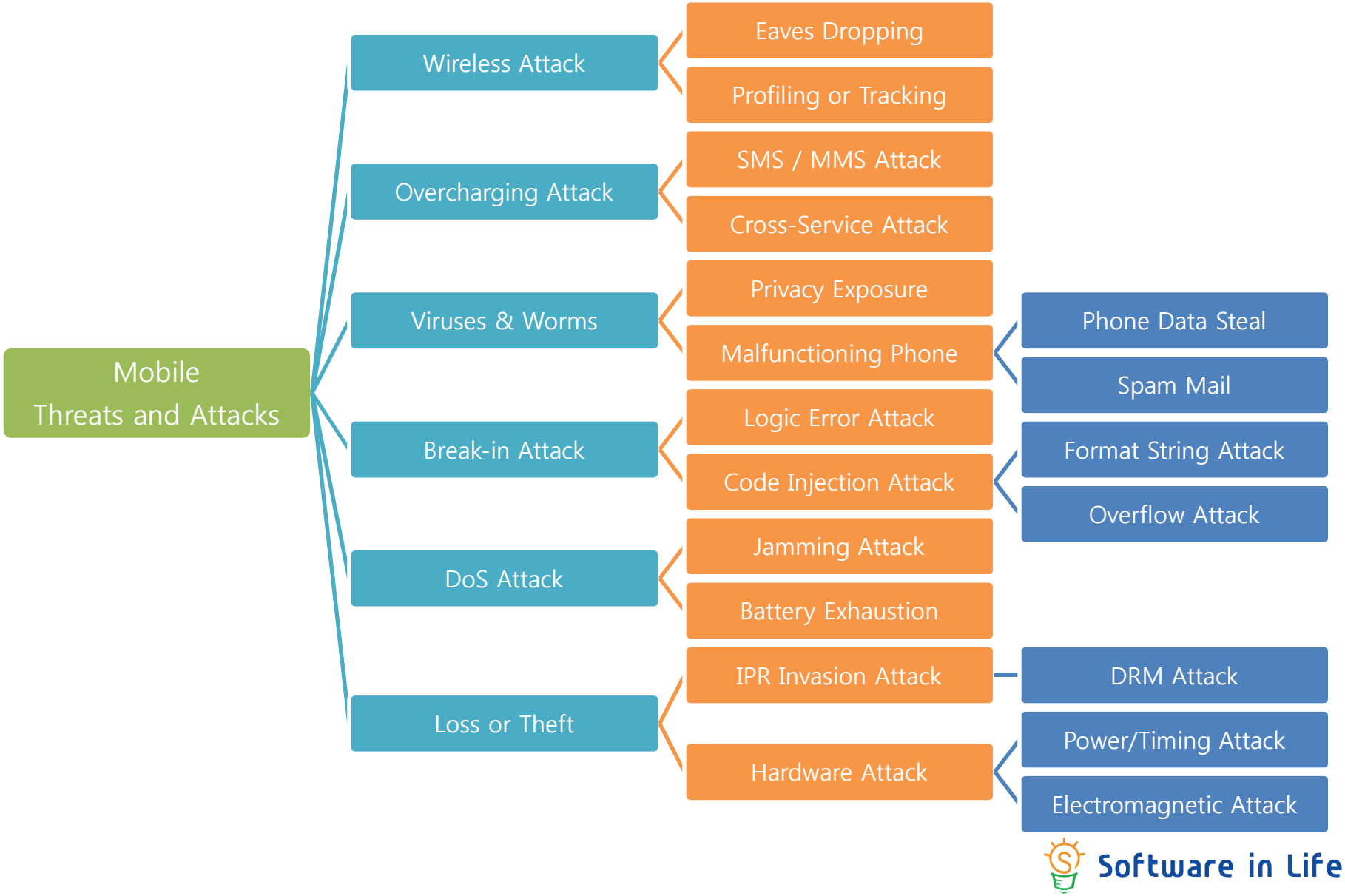
※ http://www.f-secure.com/weblog/archives/00001852.html

Mobile Security Definition

- 모바일 보안은 모바일 환경을 보호하기 위한 모든 활동을 의미함.
- 특히 최근에는 Smartphone을 중심으로 모바일 전체에 대한 보안 활동을 의미함.



Mobile Threats and Attacks



Software in Life

Mobile Threats and Attacks

이 름	유 형	특 징
피비스틸러 (PbStealer)	개인정보유출	개인 주소록의 모든 항목을 텍스트 파일 형태로 저장한 이후에 Bluetooth를 이용해 근처의 스마트폰에 무작위 전파
플렉시스파이 (FlexiSpy)	개인정보유출	사용자의 통화 기록과 SMS발송 정보를 수집하고, 해당 정보를 특정 서버에 전송하여, 사용자의 개인정보를 악의적인 목적으로 사용 가능
콤워리어 (Commwarrior)	개인정보유출	개인 주소록을 훔쳐 MMS를 통해 파일을 전송
스미싱 (SMS+phishing)	개인정보유출 과금 공격	핸드폰 사용자에게 웹사이트 링크를 포함한 문자메시지를 보낸 후 휴대폰 사용자가 웹사이트에 접속하면 트로이목마를 주입해 인터넷 사용이 가능한 휴대폰을 통제할 수 있게 됨
인포잭 (InfoJack)	개인정보유출	사용자가 모바일 기기를 인터넷에 연결할 때 설치되며, 설치된 후에는 단말기의 시리얼 정보나 운영체제 정보를 송신하고, 인증 받지 않은 파일을 설치하는 악성코드

Smartphone Security

- 고기능의 Smartphone의 보급은 모바일 보안 전체에 영향을 미치고 있음.
- Smartphone의 보안 이슈가 모바일 보안 이슈의 대부분을 차지하고 있음.

Smartphone의 출현과 변화

- **단말기술 환경의 변화**
  - PC 수준의 기능/성능을 갖춘 스마트폰 등장
  - 네트워크 인터페이스 다양화 (3G, Wi-Fi, Bluetooth, 등)
  - WIPI 의무화 해제 및 Open Platform 적용 확대
- **서비스제공 환경의 변화**
  - Open Market Place - 온라인 모바일 애플리케이션 유통 채널(환경)
  - 무선망 개방
- **유무선 통합의 촉매**
  - 모바일 오피스, 유무선 복합 서비스 등장
- **모바일 에코 시스템**
  - 기업 + 기업 or 기업 + 개인 간 자유롭고 지속적인 발전으로 상생하는 수평 관계의 커뮤니티
  - 통신사업자 + CP + 플랫폼 사업자 + 어플리케이션 개발
- **3-Screen based service**
  - PC, 휴대폰, TV의 컨텐츠 공유

Smartphone의 보안 이슈

- **단말관련 보안 이슈**
  - PC의 악성코드가 스마트폰에 재현 가능
  - 다양한 감염/침입 경로 존재
  - 단말의 개방으로 인해, 보안 취약점 노출이 급증
- **서비스 환경 관련 보안 이슈**
  - 악성코드가 포함된 모바일 애플리케이션 유통
  - 무선망에 대한 공격 가능
- **모바일 보안 이슈로의 확산**
  - 스마트폰 관련 보안 Issue는 (스마트폰을 핵심 요소로 하는) 모바일 서비스(환경)의 보안 Issue로 연결됨
  - 모바일 보안 Issue의 대부분이 스마트폰 보안 Issue와 연관됨.
  - 향후 유연한 컨텐츠 공유환경 조성에 스마트폰은 가교(bridge) 역할을 하고 있어, 현 보안 문제는 적극적으로 대응해야 할 이슈임

Smartphone Security Responsibilities

- Smartphone의 경우 다양한 이해당사자가 존재하며 과연 보안 사고가 발생하였을 경우 누가 사고의 책임이 있는가를 확인하기가 어려움.

보안 사고

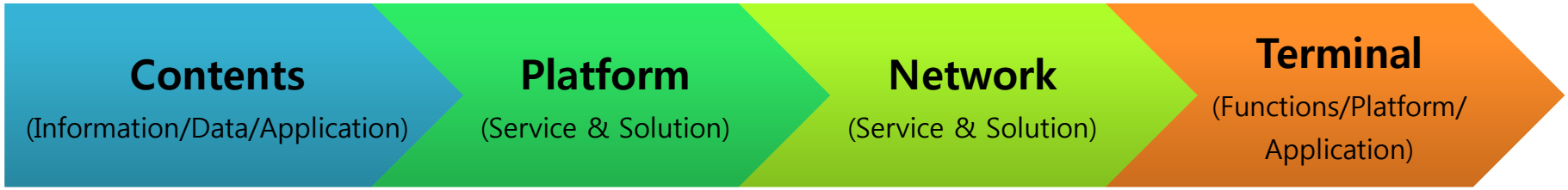
- 개인 정보 유출
- 오과금
- 좀비단말
- DoS 공격
- 오동작
- SMS 및 E-mail 발송

?

- 플랫폼 제공사
- 단말 제조사
- 이동통신사
- 어플리케이션 개발사
- 마켓 제공사
- 보안전문 기업
- 고객
- 정부

Smartphone Security Chain

- Smartphone의 Contents/Platform/Network/Terminal 각 영역별로 보안 Chain을 구성하여 대응할 필요가 있음.



악성 컨텐츠 및 App 확산 가속화	플랫폼 침해, 망 가용성 위협	네트워크 침해 위협	단말기 침해
• Open Market 유통 컨텐츠의 악성코드사전 검사 - Open-market에서 악성코드 활성화는 불특정 다수 대상의 2차 감염 발생으로 피해 확대 - 시스템화 된 자동 취약성 필터링 기능 필요	• 서비스 플랫폼의 침해는 네트워크 가용성 저해 - 다양한 멀티 서비스로 악성코드 유입 채널 다변화 - Device Management의 보안위협 감지 및 관리 필요	• Terminal 침해를 통한 무작위 SMS/MMS 발송으로 트래픽 장애 유발 - 네트워크 트래픽 점유로 가용성 저해 - 사용자에 오과금 발생방지 및 좀비 단말 점검기능 필요	• 악성코드의 탐지와 사전/사후 보안 관리 대응체계 필요 -단말기 침해만으로 도/감청 가능 - Anti-virus 이외에 추가적인 보안 S/W 필요

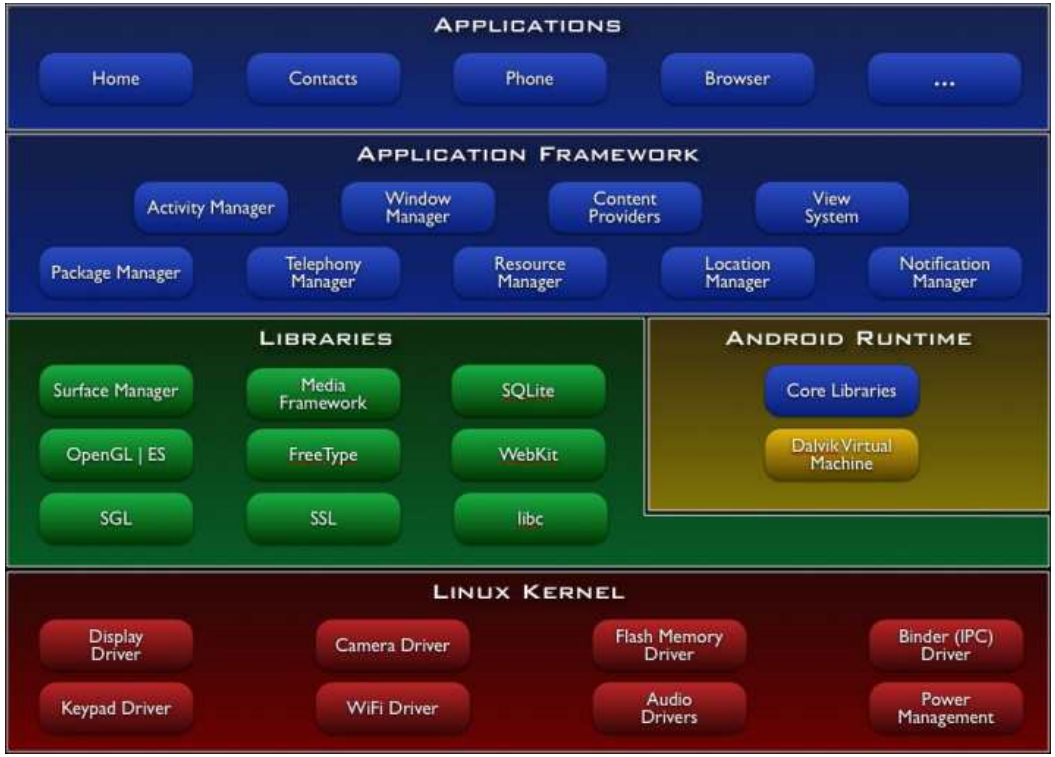
Mobile Security Platform Needs

II. Android Security

1. Android Architecture
2. Android Multitasking
3. Android Memory
4. Android Component Model
5. Android Intent
6. Android Security Model
7. Permission-based Security Model
8. Protection Levels for Permissions
9. Android User IDs and File Access
10. Android Directory
11. Android Version Control

Android Architecture

- The Android smartphone operating system is built upon Linux and includes many libraries and a core set of applications.



- Base platform
  - Linux 2.6.25 kernel
- Native Libraries
  - Libc, WebKit, etc
- Dalvik VM
  - Register-based VM
  - Runs dex bytecode
- Applications
  - Developed in Java
  - Runs on Dalvik VM
  - Linux process 1-1

Android Multitasking

What is multitasking?

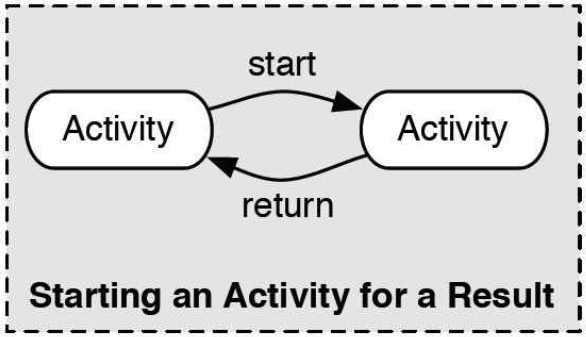
	Apple iPhone OS	Google Android	Microsoft Windows Mobile	Palm OS	Palm WebOS
OS ability to preemptively schedule multiple concurent tasks	Yes	Yes	Yes	No	Yes
Ability to use voice and data at once over the mobile network	Yes	No if CDMA (Verizon/Sprint) YES if UMTS (AT&T, TMobile)	No if CDMA (Verizon/Sprint) YES if UMTS (AT&T, TMobile)	No if CDMA (Verizon/Sprint) YES if UMTS (AT&T, TMobile)	No if CDMA (Verizon/Sprint) YES if UMTS (AT&T, TMobile)
The ability to install third party apps that run in the background	No (unless security measures are cracked)	Yes	Yes	No	Yes
The capacity for viruses and spyware to install and run in the background	No (unless security measures are cracked)	Yes	Yes	No	Yes

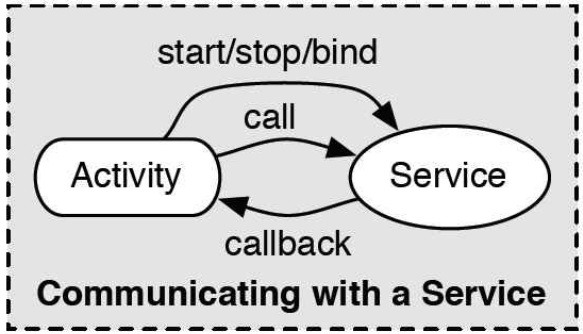
Android Memory

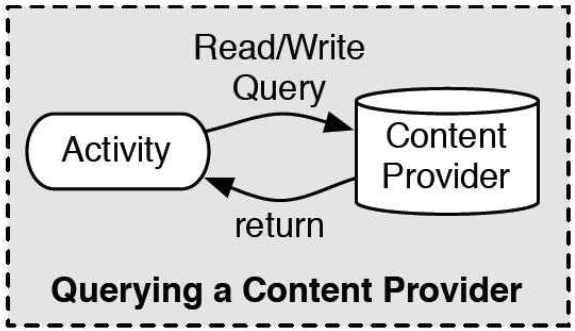
Memory types:	RAM	Storage RAM	SD Card Storage
What it does:	Built in memory for actively running apps, similar to the RAM installed in a PC.	Built in memory for storing apps and content, similar to a PC's built in hard disk.	Add-on memory for storing additional content, similar to an external PC hard disk.
Why important:	OS and running apps load here at launch, need some available RAM to operate.	OS and apps are launched from here. Limited storage means fewer or simpler apps.	This provides extra removable storage area, but can't be used to store apps for launch.
iPhone / iPhone 3G	128MB ~32MB available	8Gb to 16GB ~6,500MB available	None
iPhone 3GS	256MB ~148MB available	16Gb to 32GB ~14,500MB available	None
Android 1.x (HTC Hero)	288MB ~48MB available	256MB ~48MB available	8GB Up to 32GB cards
Android 2.x (Moto Droid)	256MB ~48MB available	512MB ~200MB available	16GB Up to 32GB cards

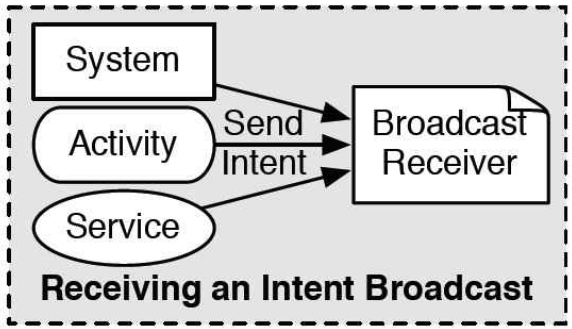
Android Component Model

- While each application runs as its own UNIX uid, sharing can occur through application-level interactions
  - Activity
  - Service
  - Content Provider
  - Broadcast Receiver









Android Intent

- Intents are objects used as inter-component signaling
  - Starting the user interface for an application
  - Sending a message between components
  - Starting a background service

- **action** -- The general action to be performed, such as ACTION_VIEW, ACTION_EDIT, ACTION_MAIN, etc.
- **data** -- The data to operate on, such as a person record in the contacts database, expressed as a Uri.

  - **ACTION_VIEW** content://contacts/people/1 -- Display information about the person whose identifier is "1".
  - **ACTION_DIAL** content://contacts/people/1 -- Display the phone dialer with the person filled in.
  - **ACTION_VIEW** tel:123 -- Display the phone dialer with the given number filled in. Note how the VIEW action does what what is considered the most reasonable thing for a particular URI.
  - **ACTION_DIAL** tel:123 -- Display the phone dialer with the given number filled in.
  - **ACTION_EDIT** content://contacts/people/1 -- Edit information about the person whose identifier is "1".
  - **ACTION_VIEW** content://contacts/people/ -- Display a list of people, which the user can browse through. This example is a typical top-level entry into the Contacts application, showing you the list of people. Selecting a particular person to view would result in a new intent { ACTION_VIEW content://contacts/N } being used to start an activity to display that person.

Android Security Model

Application signing

- All Android applications (.apk files) must be signed with a certificate whose private key is held by their developer.

Distribution of apps

- Android marketplace
- $25 signup, anyone can publish
- Non-market apps disabled by default, easy enable

Application permissions

- A basic Android application has no permissions associated with it, me aning it can not do anything that would adversely impact the user ex perience or any data on the device.

Sandboxed environment

- Each Android package (.apk) file installed on the device is given its o wn unique Linux user ID, creating a sandbox for it and preventing it fr om touching other applications (or other applications from touching i t)/

Permission-based Security Model

- Applications explicitly request pre-defined permissions

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

- Important permissions

```
<usespermission android:name="android.permission.BRICK"></usespermission>

<usespermission
android:name="android.permission.CALL_PRIVILEGED"></usespermission>

<usespermission
android:name="android.permission.DELETE_PACKAGES"></usespermission>
```

Protection Levels for Permissions

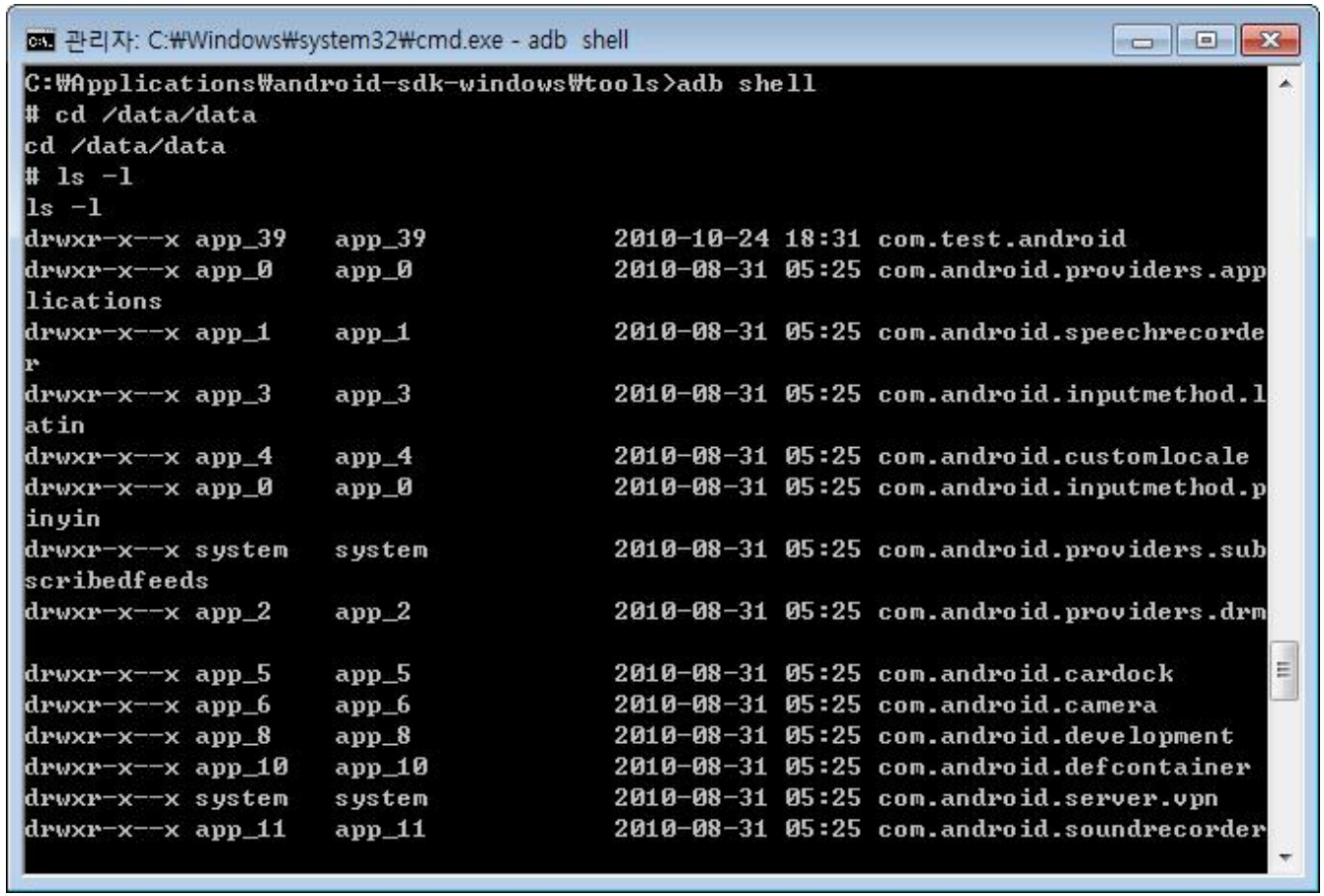
- Characterizes the potential risk implied in a permission and indicates the procedure the system should follow when determining whether to grant the permission to an application requesting it.

Constant	Value	Description
normal	0	A lower-risk permission that gives an application access to isolated application-level features, with minimal risk to other applications, the system, or the user. The system automatically grants this type of permission to a requesting application at installation, without asking for the user's explicit approval (though the user always has the option to review these permissions before installing).
dangerous	1	A higher-risk permission that would give a requesting application access to private user data or control over the device that can negatively impact the user. Because this type of permission introduces potential risk, the system may not automatically grant it to the requesting application. For example, any dangerous permissions requested by an application may be displayed to the user and require confirmation before proceeding, or some other approach may be taken to avoid the user automatically allowing the use of such facilities.
signature	2	A permission that the system is to grant only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.
signatureOrSystem	3	A permission that the system is to grant only to packages in the Android system image or that are signed with the same certificates. Please avoid using this option, as the signature protection level should be sufficient for most needs and works regardless of exactly where applications are installed. This permission is used for certain special situations where multiple vendors have applications built in to a system image which need to share specific features explicitly because they are being built together.

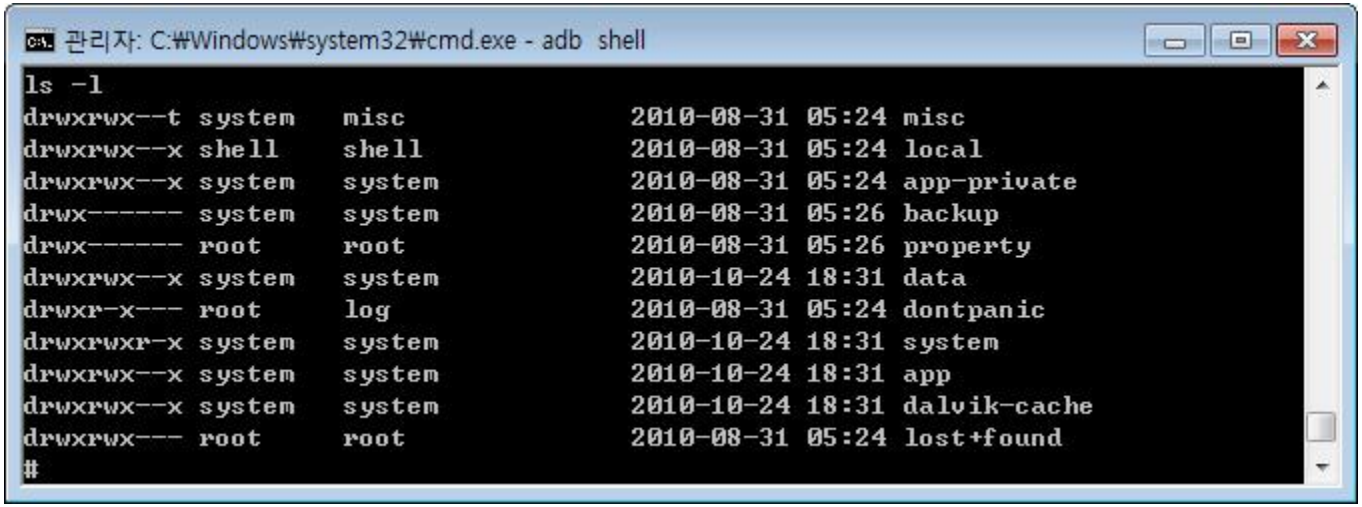
http://developer.android.com/reference/android/R.styleable.html#AndroidManifestPermission_protectionLevel

Android User IDs and File Access

- Each Android package (.apk) file installed on the device is given its own unique Linux user ID, creating a sandbox for it and preventing it from touching other applications (or other applications from touching it).

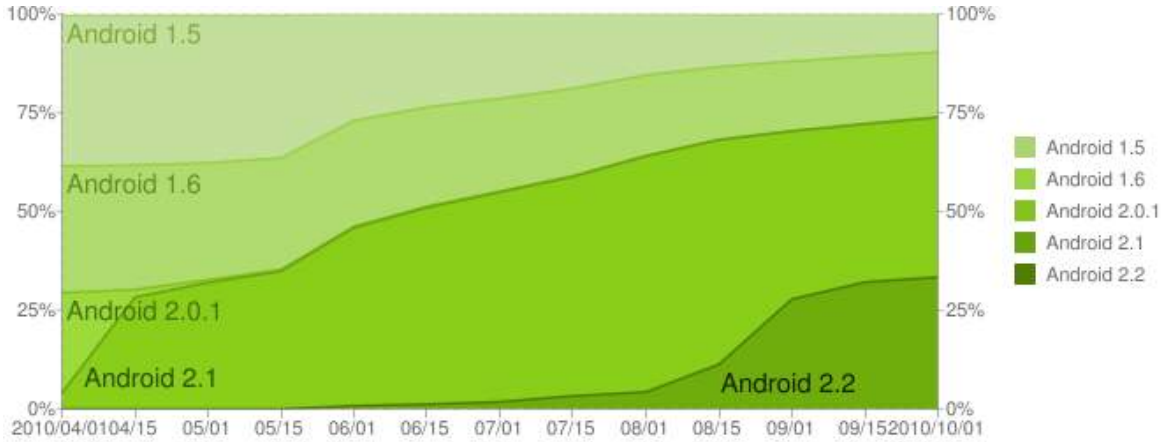


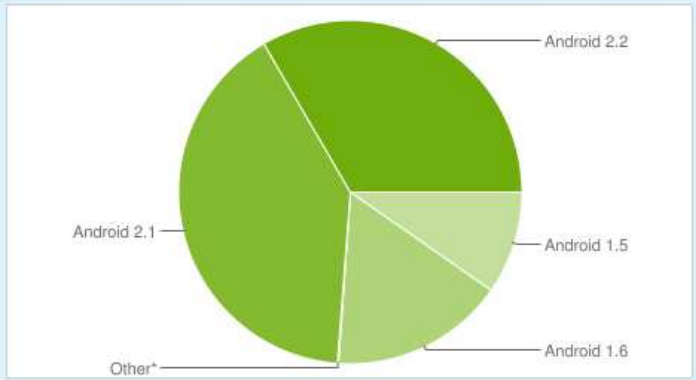
Android Directory



Directory	Description
/data	사용자 어플리케이션이 저장되는 장소
/data/app/	사용자 어플리케이션이 설치된 장소
/data/app-private	안드로이드 마켓에서 인증받은 어플리케이션이 설치된 장소
/data/data/your_package_name/	해당 어플리케이션의 라이브러리나 데이터베이스가 저장되는 장소
/system	관리 어플리케이션이 저장되는 장소
/sdcard	외부 저장 장소인 SD카드

Android Version Control





Platform	API Level	Distribution
Android 1.5	3	9.7%
Android 1.6	4	16.4%
Android 2.1	7	40.4%
Android 2.2	8	33.4%

Data collected during two weeks ending on October 1, 2010

** Other: 0.1% of devices running obsolete versions*

http://developer.android.com/resources/dashboard/platform-versions.html

Thank you!

Thank you for your interest in Software in Life Inc.
We welcome your ideas, comments, questions and requests.

Jang, Sun-Jin

E-mail: jangsunjin@softwareinlife.com
Phone: +82-10-4585-1770