Institute for Infocomm Research
A*STAR

SMU
SINGAPORE MANAGEMENT UNIVERSITY
School of Information Systems

Comparing Mobile Privacy Protection through Cross-Platform Applications

“iOS vs. Android”

Jin Han*, Qiang Yan†, Jianying Zhou*, Debin Gao†, Robert Deng†

*Institute for Infocomm Research, Singapore

†Singapore Management University

Comments from Media

Android

PCWorld

Why Android App Security Is Better Than for the iPhone

iOS

TREND MICRO

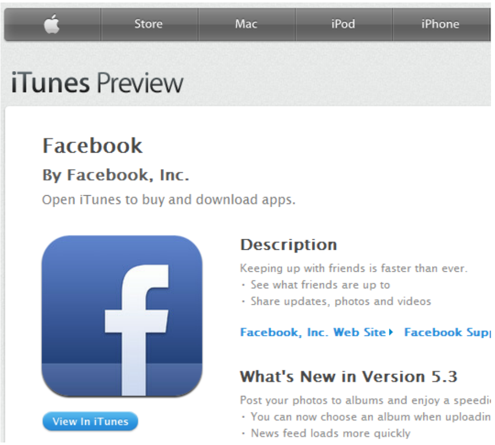
Android much less secure than iPhone

cnet

Android, iPhone security different but matched

Comparison via Cross-platform Apps

- Our solution – comparing the **cross-platform apps** running on Android and iOS:



Facebook

By Facebook, Inc.

Open iTunes to buy and download apps.

Description

Keeping up with friends is faster than ever.

- See what friends are up to
- Share updates, photos and videos

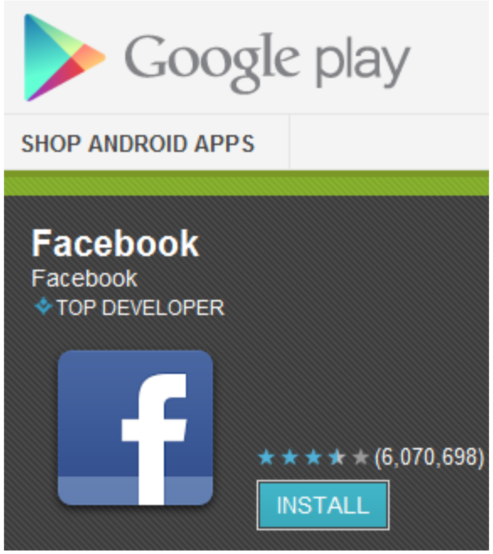
Facebook, Inc. Web Site ▸ Facebook Sup

What's New in Version 5.3

Post your photos to albums and enjoy a speedi

- You can now choose an album when uploadin
- News feed loads more quickly

vs.



  - Designed to provide the **same core functionalities**
  - Released by the same developer/company
  - Similar user interfaces and visible features

What to compare -- Usage of SS-APIs

- **S**ecurity-**S**ensitive **API**s (SS-APIs)
  - Provide access to user sensitive data
    - Contacts, Calendar, SMS, …
  - Provide access to hardware features
    - Bluetooth, Camera, Audio Recorder, Vibration …
  - Multiple **SS-APIs** → A type of SS-APIs ≈ A privilege
    - Borrow/refine the permission classification from **Android**.
- SS-API usage ≈ Privilege usage

Privileges supported by both platforms

Privilege (SS-API Type)
ACCESS_LOCATION
ACCESS_NETWORK_INFO
BATTERY_STATS
BLUETOOTH
BLUETOOTH_ADMIN
CALL_PHONE
CAMERA
CHANGE_WIFI_MULTICAST_STATE
FLASHLIGHT
INTERNET
READ_CALENDAR
READ_CONTACTS
READ_DEVICE_ID
RECORD_AUDIO
…

ACCESS_COARSE_LOCATION
ACCESS_FINE_LOCATION

SS-APIs on Android:

android.location.LocationManager.**addGpsStatusListener()**

android.location.LocationManager.getProvider()

android.telephony.TelephonyManager.**getCellLocation()**

android.telephony.TelephonyManager.getNeighboringCellInfo()

android.webkit.GeolocationService.setEnableGps()

…

SS-APIs on iOS:

[CLLocationManager startUpdatingLocation]

[CLLocationManager startMonitoringSignificantLocationChanges]

[CLLocationManagerDelegate
locationManager:didUpdateToLocation:fromLocation:]

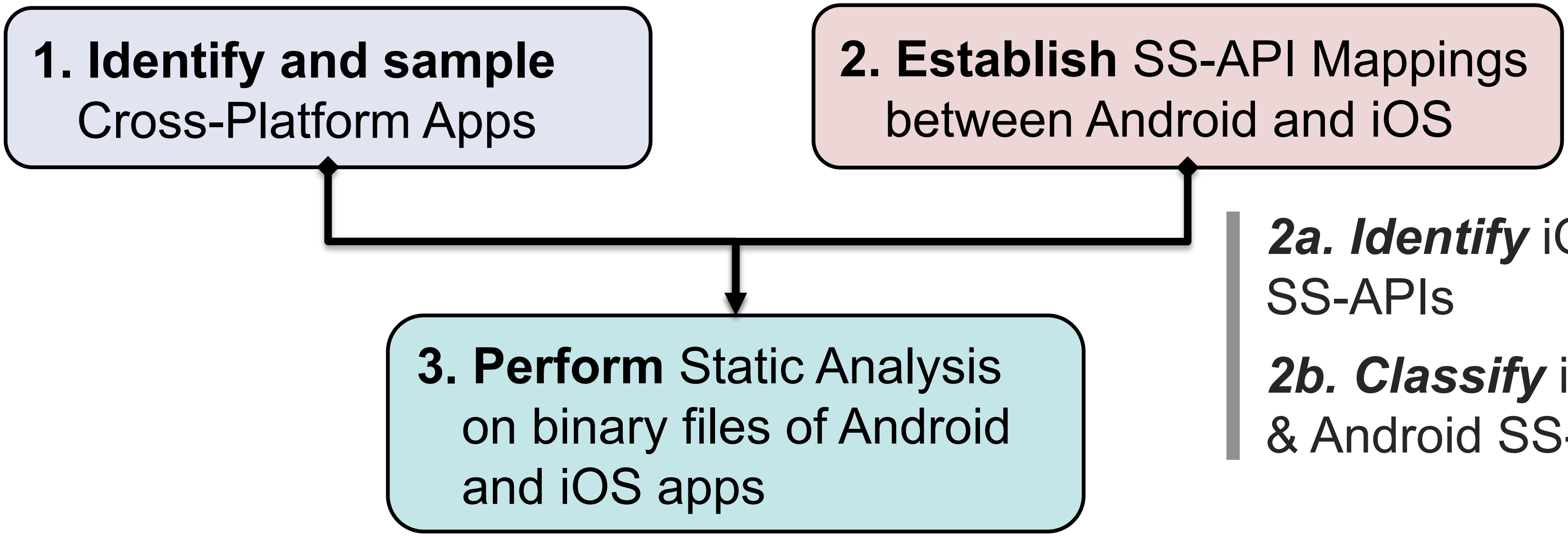
MKUserLocation.location

…

Methodology Overview

1a. Web crawlers for Google Play (300,000) and iTunes Store (400,000)

1b. App matcher based on information retrieval techniques



1. Identify and sample Cross-Platform Apps

2. Establish SS-API Mappings between Android and iOS

3. Perform Static Analysis on binary files of Android and iOS apps

2a. Identify iOS SS-APIs

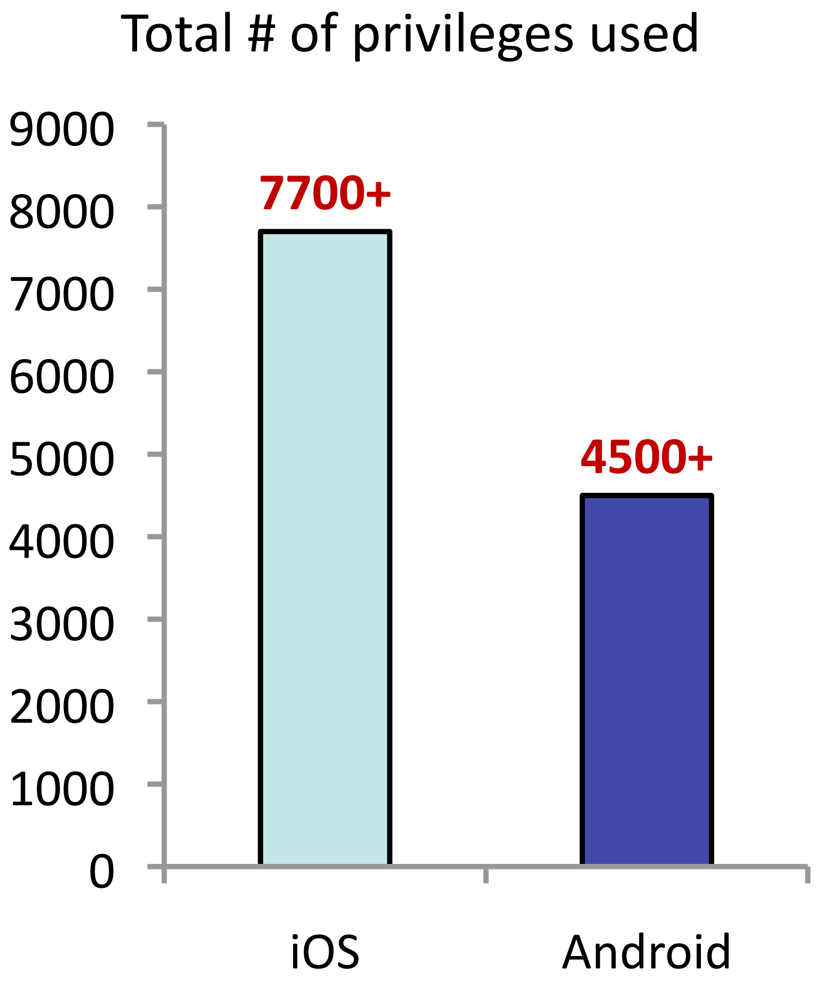
2b. Classify iOS & Android SS-APIs

3a. Static Analysis Tool for **iOS** Objective-C Executable

3b. Static Analysis Tool for **Android** Dalvik Bytecode

***3c.* SS-API analyzer** for SS-API separation and comparisons

Results at First Glance



For **1300** pairs of **popular** free *cross-platform apps*:

- Certain privileges (**INTERNET**, **BLUETOOTH**) are required almost equally.
- Many other privileges are required very **differently**.
- **948 (73%)** of iOS apps access **additional** privileges compared to its Android version.

Privilege Usage Difference

Privilege	# of Android Apps	# of iOS Apps	Only on iOS
READ_DEVICE_ID	510	925	469
CAMERA	172	601	435
VIBRATE	374	522	290
ACCESS_NETWORK_INFO	885	1065	269
READ_CONTACTS	151	388	256
SEND_SMS	29	264	248
⋮	⋮	⋮	⋮
READ_CALENDAR	35	174	141

- iOS apps usually access more privileges than Android apps, which are often associated with accessing sensitive resources such as device ID, camera, and users' contacts.

Case #1: Angry Birds

- The almighty game by Rovio
  - requires **READ_CONTACTS** on iOS
- API call ABAddressBookGetPersonWithRecordID observed in the code section of **CCPrivateSession**. getArrayOfAddressBookEmailAddressesNamesAndContactIDs

Still exist until version 2.1.0
(released in March 2012)

Removed on version 2.2.0
(released in August 2012)

Case #2: Words With Friends

- A famous game app by Zynga
  - iOS version requires **13** privileges.
  - Android version only requires **6**.

- The additional privileges on iOS:
  - **BATTERY_STATS**
    API call UIDevice.setBatteryMonitoringEnabled in the code region of **MMManager**.handshakeURL [Millennial Media]
  - **CALL_PHONE**
    UIApplication.openURL with "tel:" parameter in **IMAdView**.placeCallTo and other locations
  - **CAMERA**
    UIImagePickerController.setSourceType is observed in **MobclixRichMediaWebAdView**.takePhotoAndReturnToWebview

Investigation #1: Third-Party Libraries

- Privilege Usage of Third-Party Libraries
  – We identified commonly used third-party libraries on both Android (**79** libraries) and iOS (**72** libraries).

Library Name	Android App Ratio	iOS App Ratio	SS-API Types on Android	SS-API Types on iOS
Google Ads	21.7 %	15.9 %	ANI, INT	ANI, INT, RDI, SMS, VIB, WAK
Flurry	19.1 %	19.9 %	LOC, INT	LOC, INT, RDI
Millennial Media	7.3 %	9.3 %	ANI, INT, RDI	LOC, ANI, CAM, INT, CON, RDI, VIB
AdWhirl	3.8 %	6.9 %	LOC, INT	LOC, ANI, INT, RDI
Mobclix	3.2 %	3.7 %	LOC, ANI, INT, RDI	LOC, ANI, BAT, CAM, FLA, INT, CAL, CON, RDI, SMS, VIB

Investigation #2: Apps' Own Code

- Corresponding security sensitive APIs may also be accessed by the App's own code.

Privilege	**Exclusively caused by Lib**	**Exclusively caused by App**	**Caused by both Lib & App**
READ_DEVICE_ID	36%	40%	24%
CAMERA	27%	62%	11%
VIBRATE	54%	38%	8%
ACCESS_NETWORK_INFO	4%	86%	10%
READ_CONTACTS	25%	48%	27%
SEND_SMS	32%	51%	17%
⋮	⋮	⋮	⋮
READ_CALENDAR	33%	65%	2%

** This table shows the usage pattern for those **extra** privileges **only** used in iOS apps.*

Possible Explanation #1

- **Functional difference**
  - `ACCESS_NETWORK_INFO`
    - Caused by the implementation difference on the Reachability test by analyzing several open-source apps.
  - `CAMERA`
    - OpenFeint library on iOS and Android:
      - Use `CAMERA` **only on iOS**, for setting profile photos.
      - Every game with OpenFeint enabled would require `CAMERA` privilege.

Possible Explanation #2

- **Intentional avoidance**
  - *WordPress* app on Android obtains UUID differently compared to its iOS version
  - The programmers intentionally avoid triggering `READ_PHONE_STATE` on Android.
  - Confirmed by consulting WordPress developers:

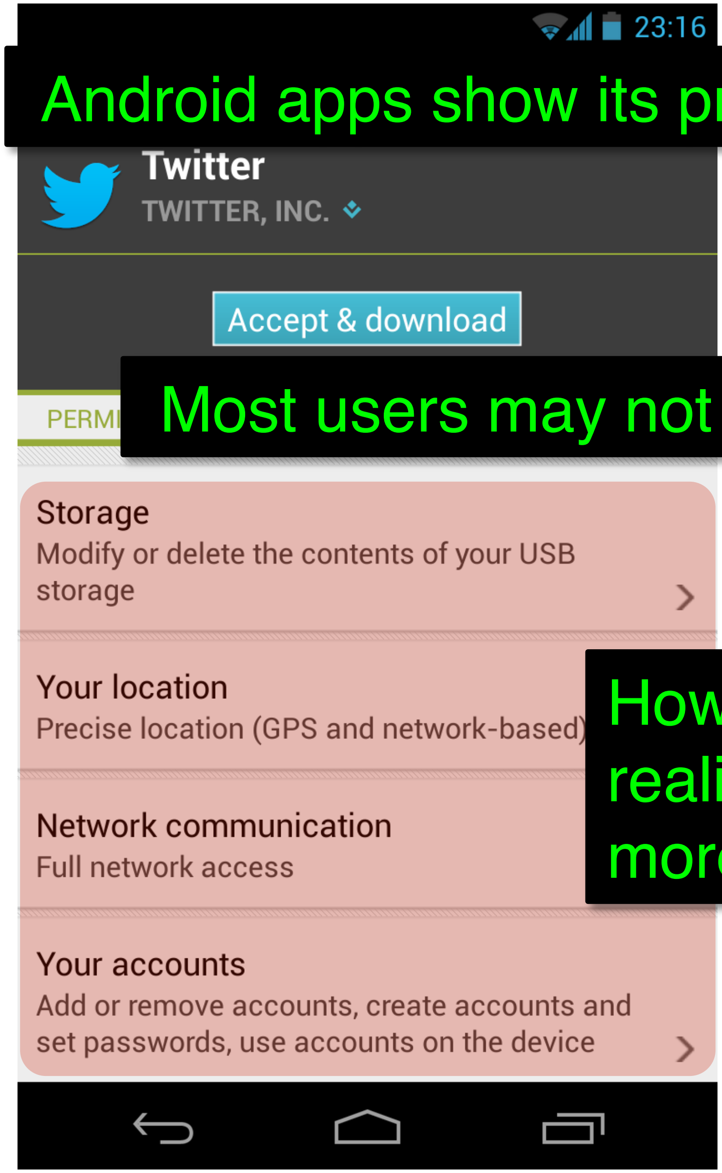
“*… because it doesn’t require that permission which* ***reads quite poorly*** *as ‘read phone state and identity’ …*”

The Implication

Android apps show its privilege list before installation

Most users may not read/understand this privilege list…

However, as long as the app developers realize someone may read it, they become more **cautious** in requesting privileges.



23:16

Twitter

TWITTER, INC.

Accept & download

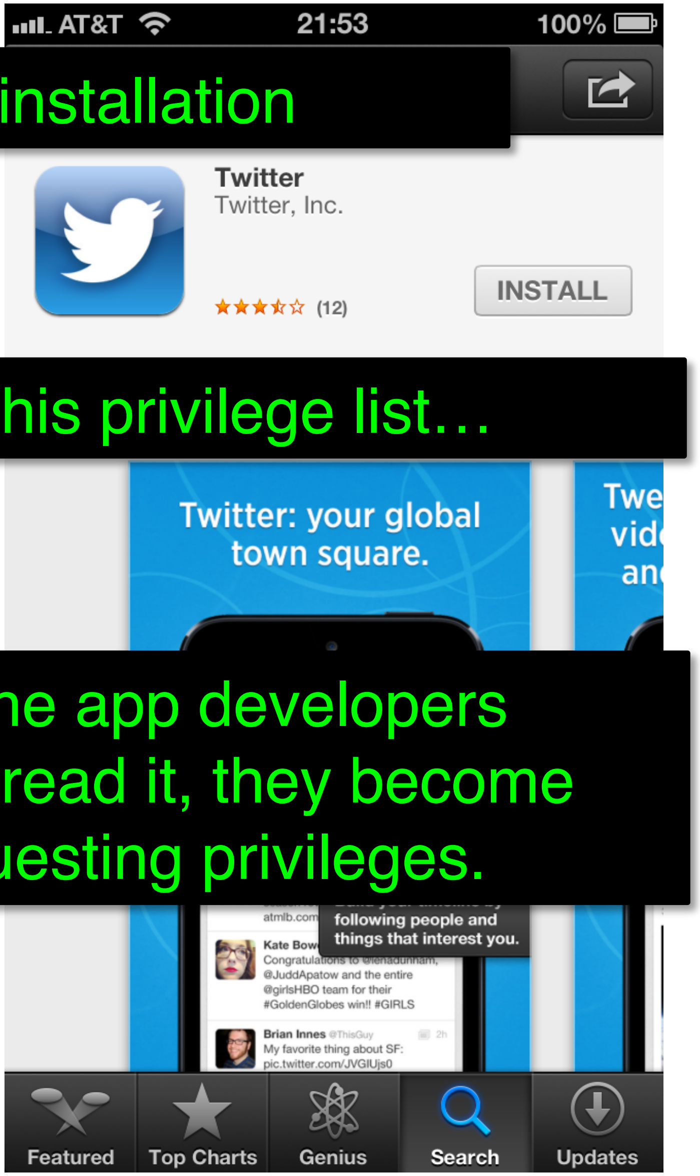
PERMI

Storage
Modify or delete the contents of your USB storage

Your location
Precise location (GPS and network-based)

Network communication
Full network access

Your accounts
Add or remove accounts, create accounts and set passwords, use accounts on the device



AT&T 21:53 100%

Twitter
Twitter, Inc.

★★★★☆ (12)

INSTALL

Twitter: your global town square.

atmlb.com

following people and things that interest you.

Kate Bow
Congratulations to @lenadunham, @JuddApatow and the entire @girlsHBO team for their #GoldenGlobes win!! #GIRLS

Brian Innes @ThisGuy 2h
My favorite thing about SF: pic.twitter.com/JVGIUjs0

Evolution on iOS

- The original comparison was performed on **iOS 5.0** and **Android 4.0**
  - On **iOS 5**, only two privileges are shown to user:
    - access location info & send push notifications
  - Since **iOS 6**, more privileges can be controlled:
    - access to contacts, calendar, photos and reminders.
- Such changes have impacts on privilege usage:
  - 48.7% (633/1300) apps released updates since Aug, 2012.
  - **18%** iOS apps originally require **`READ_CONTACTS`** have **removed** this privilege in their new versions.
  - **16%** **removed** for **`READ_CALENDAR`** privilege.

Evolution on iOS

- The original comparison was performed on **iOS 5.0** and **Android 4.0**
  - On **iOS 5**, only two privileges are shown to user:
    - access location info & send push notifications
  - Since **iOS 6**, more privileges can be controlled:
    - access to contacts, calendar, photos and reminders.
- Such changes have impacts on privilege usage:
  - API call ABAddressBookGetPersonWithRecordID observed in AngryBirds
  - Still exist until version 2.1.0 (Mar 2012)
  - **Removed** from version 2.2.0 (Aug 2012)

Conclusion

- This work is the **first attempt** to establish a baseline on **systematic comparison between** Android and iOS, which shows how the platform difference affects the behavior of **cross-platform apps**.
- Our results show
  - iOS apps turn to access more **Security-Sensitive APIs**, which are related to sensitive resources such as device ID, contacts and calendar.
  - Caused by both **third-party libraries** and **apps' own code**.
  - A strong correlation exists between the **usage** difference of **privileges** and the **availability** of **privilege-list** mechanism on Android and iOS.

[redacted]

iOS vs. Android ?

Security Feature	Android	iOS
Permission Notification	Yes	**Little**
Approval/Vetting Process	**Partial**	Yes
Binary Encryption	Since v4.1	Yes

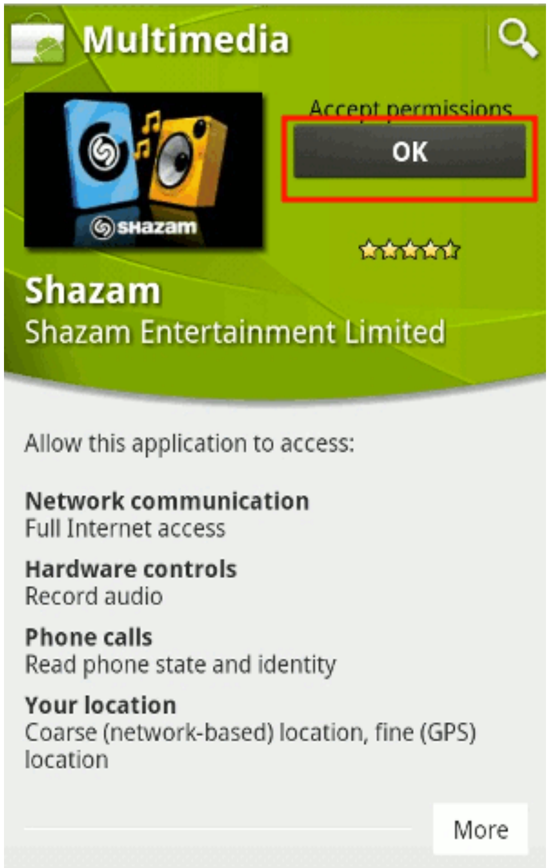
- Android – open source platform
- iOS – closed source platform

- **How to compare?**

Android permission classification

Group of Privileges	# of Privileges	SS-API Type Examples
Not actually exist in Android	7	SET_PREFERRED_APPLICATIONS BRICK
Reserved for System or OEMs	42	DELETE_CACHE_FILES WRITE_SECURE_SETTINGS
Not supported by iOS	46	CHANGE_NETWORK_STATE MODIFY_AUDIO_SETTINGS
Supported by both Android and iOS	**20**	BLUETOOTH READ_CONTACTS RECORD_AUDIO
Total	115	

Android Permission Notification



Shazam

Shazam Entertainment Limited

Allow this application to access:

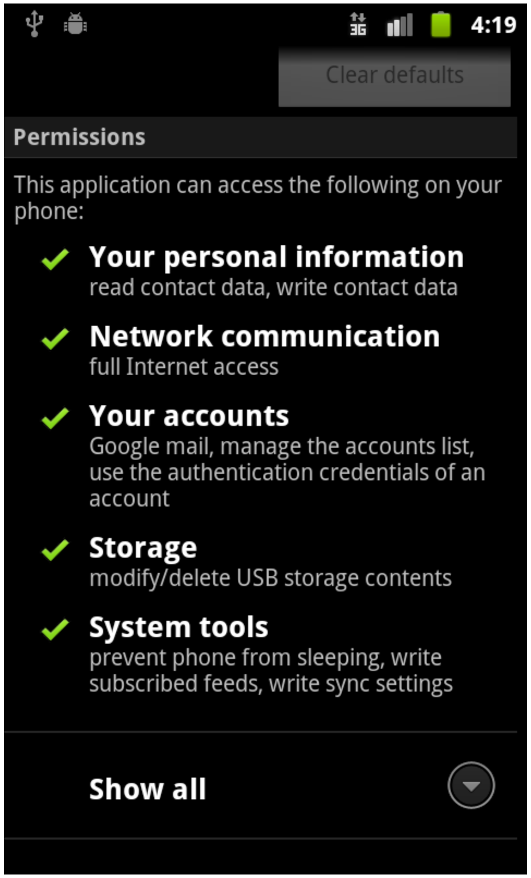
Network communication
Full Internet access

Hardware controls
Record audio

Phone calls
Read phone state and identity

Your location
Coarse (network-based) location, fine (GPS) location

A music player

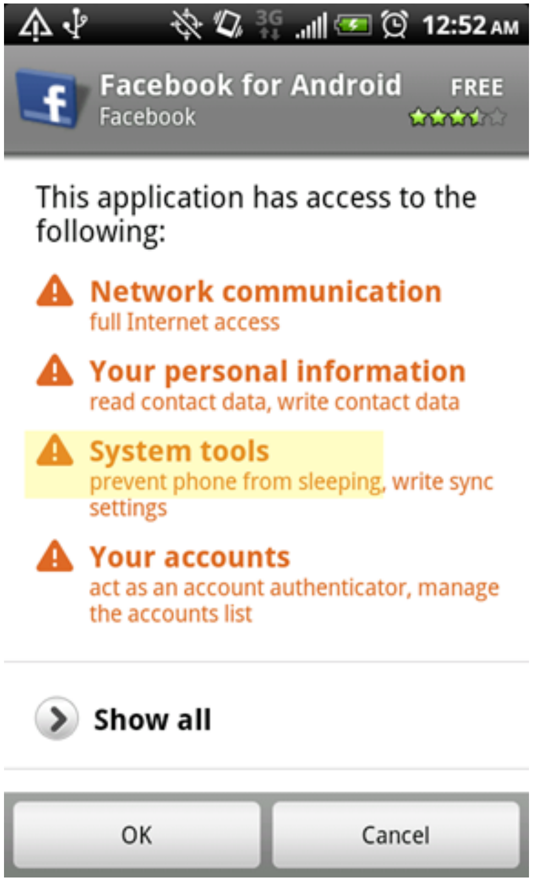


Permissions

This application can access the following on your phone:

- ✓ **Your personal information**
  read contact data, write contact data
- ✓ **Network communication**
  full Internet access
- ✓ **Your accounts**
  Google mail, manage the accounts list, use the authentication credentials of an account
- ✓ **Storage**
  modify/delete USB storage contents
- ✓ **System tools**
  prevent phone from sleeping, write subscribed feeds, write sync settings

Gmail



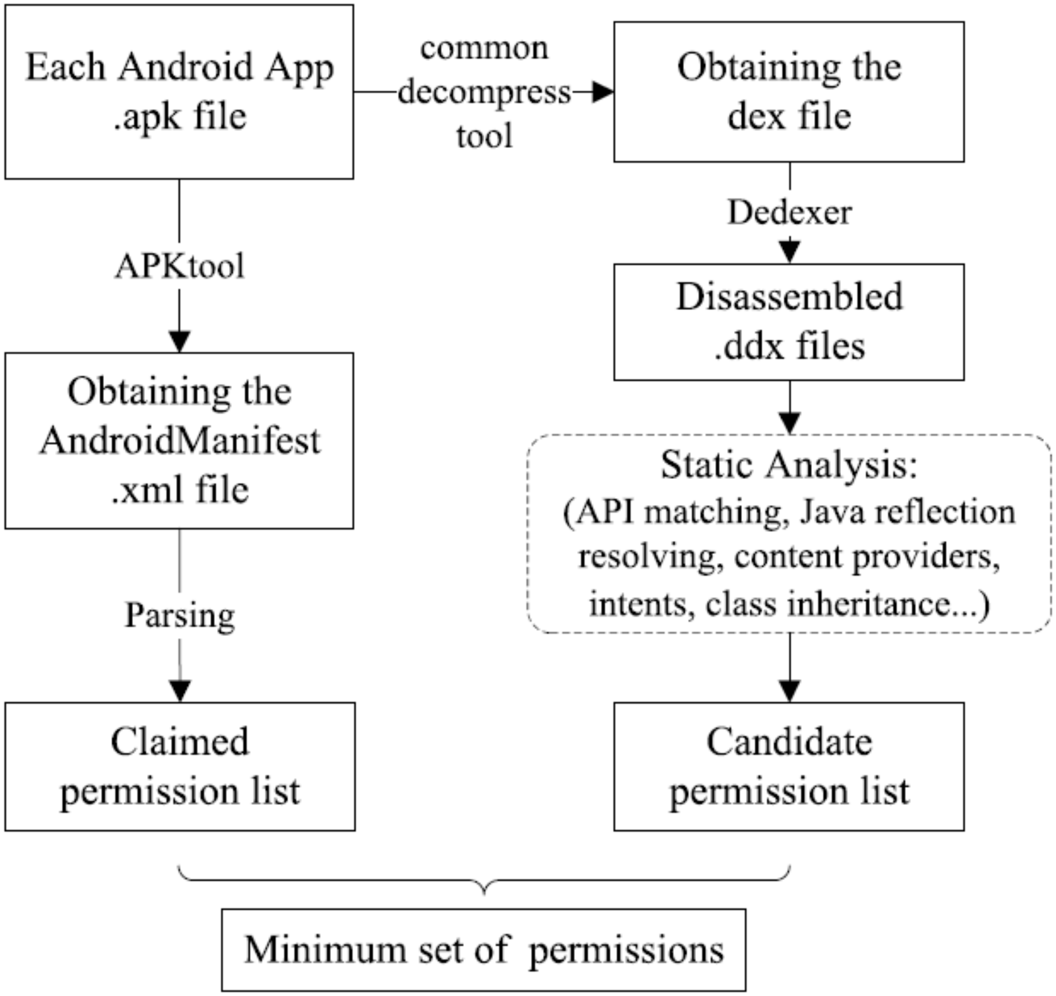
This application has access to the following:

- ⚠ **Network communication**
  full Internet access
- ⚠ **Your personal information**
  read contact data, write contact data
- ⚠ **System tools**
  prevent phone from sleeping, write sync settings
- ⚠ **Your accounts**
  act as an account authenticator, manage the accounts list

Facebook

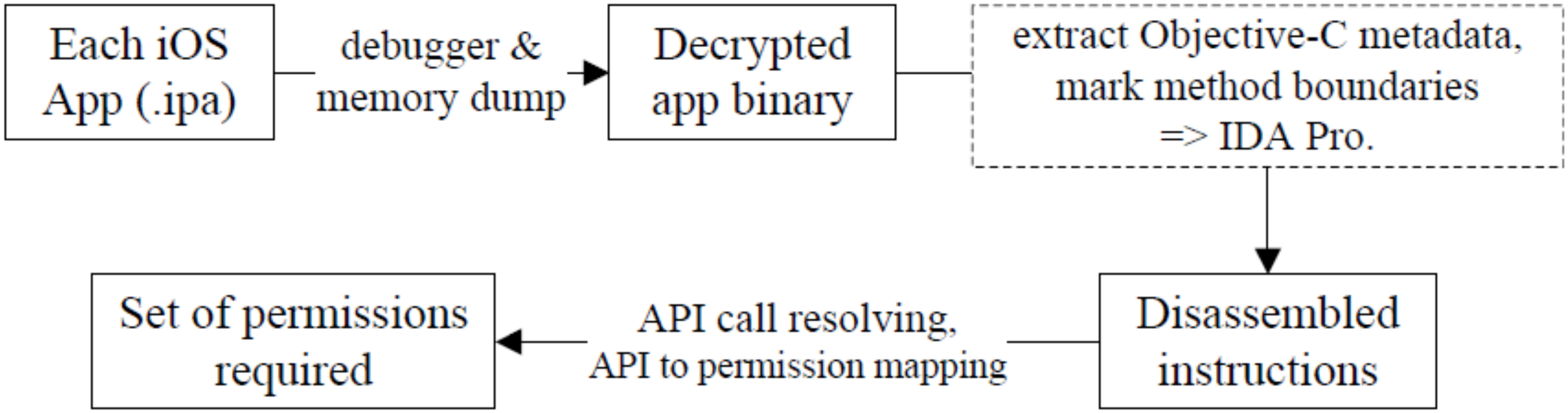
Android App Static Analysis Tool

- Class inheritance
- **Java reflection resolving**
- Content provider
- Intents


Each Android App .apk file
common decompress tool
Obtaining the dex file
Dedexer
APKtool
Disassembled .ddx files
Obtaining the AndroidManifest .xml file
Static Analysis: (API matching, Java reflection resolving, content providers, intents, class inheritance...)
Parsing
Claimed permission list
Candidate permission list
Minimum set of permissions

iOS App Static Analysis Tool

- iOS static analysis tool:
  - App decryption/cracking
  - Method boundaries marking
  - **`Objc_msgSend`** resolving


Each iOS App (.ipa)
debugger & memory dump
Decrypted app binary
extract Objective-C metadata, mark method boundaries => IDA Pro.
Disassembled instructions
API call resolving, API to permission mapping
Set of permissions required