STORAGE AND PERMISSIONS – 14.1

**Q1. What is the difference between Internal Storage & External Storage?**

- When building an app that uses the internal storage, the Android OS creates a unique folder, which will only be accessible from the app, so no other app, or even the user, can see what's in the folder. The external storage is more like a public storage, so for now, it's the sdcard, but could become any other type of storage (remote hard drive, or anything else).

The internal storage should only be used for application data, (preferences files and settings, sound or image media for the app to work). If you intent to download many mp3s, saving them to external storage will be safe as the external storage is often bigger. Besides, storing data on the internal storage may prevent the user to install other applications.

**Q2. For how long the data resides in the cache?**

- Typically files will stay in the cache until space runs out. It depends upon the browser settings. But note that having a file cached doesn't necessarily mean that changes are not fetched from your site. If configured to do so, the browser will send a request to the server, with details about the date of the cache file. The server than then respond with "ok, use your cache - it's the latest version" when there are no changes. This response is small and quickly sent. If the server version has been updated, then the server will respond with the new version.

**Q3. What are the critical Permissions and Normal Permissions? What are the examples of each?**

**Normal Permissions:**

- Many permissions are designated as PROTECTION\_NORMAL, which indicates that there's no great risk to the user's privacy or security in letting apps have those permissions. For example, users would reasonably want to know whether an app can read their contact information, so users have to grant this permission explicitly. By contrast, there's no great risk in allowing an app to vibrate the device, so that permission is designated as normal.

If an app declares in its manifest that it needs a normal permission, the system automatically grants the app that permission at install time. The system does not prompt the user to grant normal permissions, and users cannot revoke these permissions.

As of API level 23, the following permissions are classified as PROTECTION\_NORMAL:

ACCESS\_LOCATION\_EXTRA\_COMMANDS

ACCESS\_NETWORK\_STATE

ACCESS\_NOTIFICATION\_POLICY

ACCESS\_WIFI\_STATE

BLUETOOTH

BLUETOOTH\_ADMIN

BROADCAST\_STICKY

CHANGE\_NETWORK\_STATE

CHANGE\_WIFI\_MULTICAST\_STATE

CHANGE\_WIFI\_STATE

DISABLE\_KEYGUARD

EXPAND\_STATUS\_BAR

GET\_PACKAGE\_SIZE

INSTALL\_SHORTCUT

INTERNET

KILL\_BACKGROUND\_PROCESSES

MODIFY\_AUDIO\_SETTINGS

NFC

READ\_SYNC\_SETTINGS

READ\_SYNC\_STATS

RECEIVE\_BOOT\_COMPLETED

REORDER\_TASKS

REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS

REQUEST\_INSTALL\_PACKAGES

SET\_ALARM

SET\_TIME\_ZONE

SET\_WALLPAPER

SET\_WALLPAPER\_HINTS

TRANSMIT\_IR

UNINSTALL\_SHORTCUT

USE\_FINGERPRINT

VIBRATE

WAKE\_LOCK

WRITE\_SYNC\_SETTINGS

**Critical permissions:**

READ\_CALENDAR

WRITE\_CALENDAR

CAMERA

READ\_CONTACTS

WRITE\_CONTACTS

GET\_ACCOUNTS

ACCESS\_FINE\_LOCATION

ACCESS\_COARSE\_LOCATION

RECORD\_AUDIO

READ\_PHONE\_STATE

CALL\_PHONE

READ\_CALL\_LOG

WRITE\_CALL\_LOG

ADD\_VOICEMAIL

USE\_SIP

PROCESS\_OUTGOING\_CALLS

BODY\_SENSORS

SEND\_SMS

RECEIVE\_SMS

READ\_SMS

RECEIVE\_WAP\_PUSH

RECEIVE\_MMS

READ\_EXTERNAL\_STORAGE

WRITE\_EXTERNAL\_STORAGE