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

**Internal Storage:**

It is not accessible by the user, except by installed apps or by rooting the Android device. The visibility of data stored in this storage is public.

Any files stored in the internal storage are private to the applications. Other applications cannot access them. These files are deleted when users uninstall the application that creates and uses them.

**External Storage:**

This can be a removable storage media (SD card) or non-removable (internal) storage and can be accessed by the user. It is also accessible by the user by using file manager apps. The visibility of data stored in this storage is public.

There's no security enforced upon files you save to the external storage. Any files stored in the external storage are publicly available to other applications. These files can be deleted by other applications or by the user. These files are not deleted when users uninstall the application.

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

Data in cache remains until it is deleted under 2 circumstances. They are:

1. When the device is low on internal storage space, Android may delete cached files to recover space or the user explicitly requests system to delete the cache data.
2. When the application (as decided by the app developer) decides to delete the cached files.
3. **What are the critical Permissions and Normal Permissions? What are the examples of each?**

**Normal permissions** are permissions for which there is no great risk to user’s privacy or security when enabled. If an app declares that it needs a normal permission, in the manifest file, then system automatically grants the permission to the app.

Example:

ACCESS\_NETWORK\_STATE,

ACCESS\_WIFI \_STATE,

CHANGE\_NETWORK\_STATE,

DISABLE \_KEYGUARD

CHANGE\_WIFI\_STATE

GET\_PACKAGE\_SIZE etc.

**Critical Permissions or Dangerous Permissions** are permissions which are used when an app wants access to data or resources that involve the user’s private information, or affect user’s stored data, system’s integrity or the operation of other apps. If an app declares that it needs a dangerous permission, in the manifest file, then the permission is granted to the app only after the user approves of it explicitly at runtime.

Example:

READ\_CALL\_LOG,  
 READ\_CONTACTS,  
 READ\_EXTERNAL\_STORAGE,  
 READ\_CALL\_LOG,  
 READ\_CONTACTS,  
 READ\_EXTERNAL\_STORAGE,  
 READ\_CONTACTS,  
 READ\_SMS,  
 RECEIVE\_SMS,  
 SEND\_SMS,  
 WRITE\_CALENDAR etc.