Session 14: Saving Data & Working with System Permissions

Assignment: Saving Data and Permissions

a) What is the difference between Internal Storage & External Storage?

Internal storage of an Android phone is partitioned into two parts - Internal Storage and Phone Storage. And external storage often refers to the SD card or USB drivers that are inserted/plugged into the phone.

Internal Storage also called System Memory is used to store the operating system, system apps, and other app data (messages, contacts, email settings, and other personal information). It is the space that can actually be accessed and used by the users, and is the default location for installed apps, games, camera photos, downloaded music and media files.

External storage generally means removable microSD card **that is inserted into the phone to add extra space to the phone. External storage is used to save media files such as pictures, music, videos etc. However, most applications cannot be installed on external storage.**

b) For how long the data resides in the cache?

Cached data of a website or an app is information that is stored on computer, smart phone or a tablet. This cached data is stored on devices so that during the next time of its use, it will readily be available. But, downside of this cached data is that, it takes up space on the device, which means it need to clear cached data every now and again.

Hence, data residing in the cache depends on person, browser and settings. Browsers usually reserve a certain amount of disk space. If a user stops using the browser it resides indefinitely. If he/she uses the browser rarely, it will reside till the expiration - either by internal policy or by HTTP headers. If he/she uses the browser heavily, it can be 12 minutes or even less. If the target audience site is users who use their browsers heavily, it can be very short. On the other hand if your site is only website visited it can be nearly never. It implies that how long data resides in the cache will depend on person, browser and settings.

c) What are the critical Permissions and Normal Permissions? What are the examples of each?

Permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS) as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.

Normal **permissions cover areas where an app needs to access data or resources outside the app's sandbox subject to little risk to the user's privacy or the operation of other apps.**

For example, permission to set the time zone is a normal permission. 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 doesn't prompt the user to grant normal permissions, and users cannot revoke these permissions.

Dangerous or critical permissions are checked at runtime. These permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps.

For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. Until the user approves the permission, app cannot provide functionality that depends on that permission. To use a dangerous permission, app must prompt the user to grant permission at runtime.