Assignment 14.1

|  |
| --- |
|  |
|  |
|  | 1. What is the difference between Internal Storage & External Storage?   Ans. External storage is outside the computer enclosure. Internal is inside. External storage sometimes needs an additional power source, internal is connected to the computer power supply. External storage can use the same sort of connection (SATA) as internal, but it frequently just uses USB as that is more common. |
|  | Internal storage is seen as an integral part of your computing device. External storage is something you add on. |
|  | External storage sometimes needs a drive controller while internal operates using components on the motherboard. |
|  | "Internal" storage refers to the media contained within the box -- usually Hard Drives. |
|  | "External" storage refers to the media connected from the outside of the box (usually by USB or eSATA). |
|  | Internal is inside the computer,usually soldered or integrated in some chip, not user accessible. |
|  | External is outside or pluggable, user accessible. |
|  |  |
|  |  |
|  | (b) For how long the data resides in the cache? |
|  | Ans. Cache memory is dynamic memory for data storing. when OS is ordered to perform some work, then data related to that work will be taken to cache memory before executing the task. This data will reside in the cache until new data overrides it. |
|  |  |
|  |  |
|  | (c) What are the critical Permissions and Normal Permissions? What are the examples of each? |
|  | Ans. Normal Permission::-  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. |
|  | Ex. ACCESS\_LOCATION\_EXTRA\_COMMANDS |
|  | ACCESS\_NETWORK\_STATE |
|  | ACCESS\_NOTIFICATION\_POLICY |
|  | ACCESS\_WIFI\_STATE |
|  | BLUETOOTH |
|  | BLUETOOTH\_ADMIN |
|  | BROADCAST\_STICKY |
|  | CHANGE\_NETWORK\_STATE |
|  |  |
|  | External Permission ::-  Many permissions which indicates that there's great risk to the user's privacy or security in letting apps have those permissions. For example, users would reasonably want to enter the app so users have to grant this permission explicitly. By contrast, there's great risk in allowing an app to vibrate the device, so that permission is designated as critical. If an app declares in its manifest that it needs a critical permission, the system automatically checks the app that permission at install time. The system does not allow the user to grant critical permissions without checking. |
|  | Ex. READ\_CALENDAR |
|  | WRITE\_CALENDAR |
|  | CAMERA |
|  | READ\_CONTACTS |
|  | WRITE\_CONTACTS |
|  | GET\_ACCOUNTS |
|  | ACCESS\_FINE\_LOCATION |
|  | ACCESS\_COARSE\_LOCATION |
|  | RECORD\_AUDIO . |