access control in android marshmallow

BY

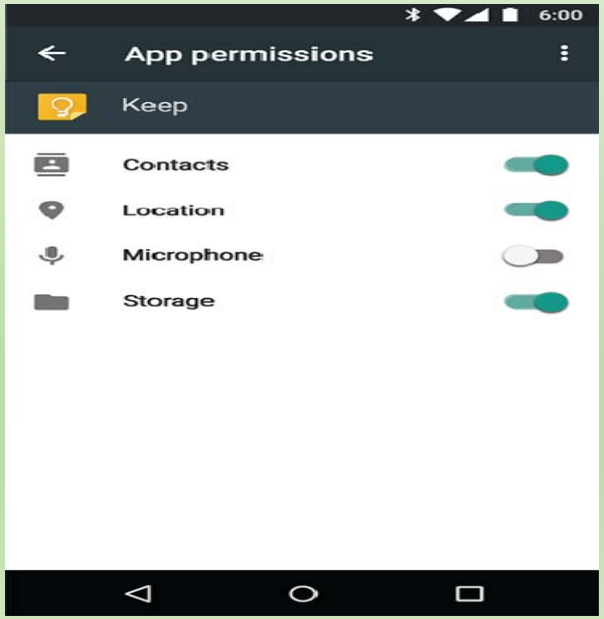
BAHAAULDDIN NABHAN

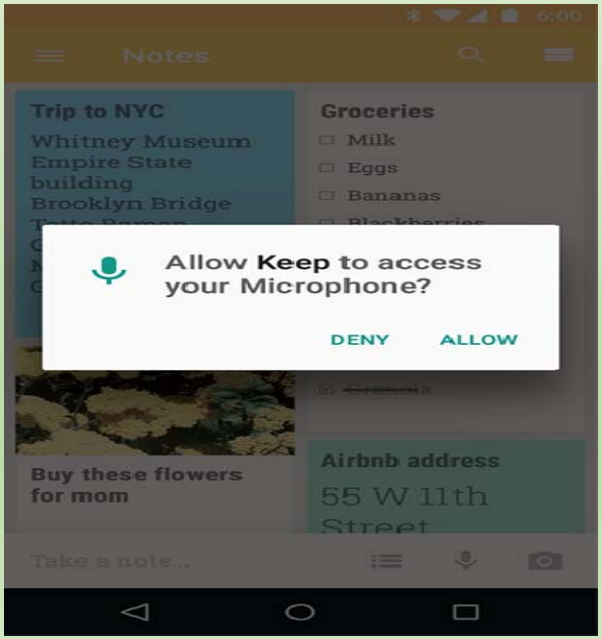
What is android marshmallow

- **Android "Marshmallow"** (codenamed **Android M** during development) is the sixth major version of the Android operating system. First released as a beta build on May 28, 2015, it was officially released on October 5, 2015, with Nexus devices being the first to receive the update.

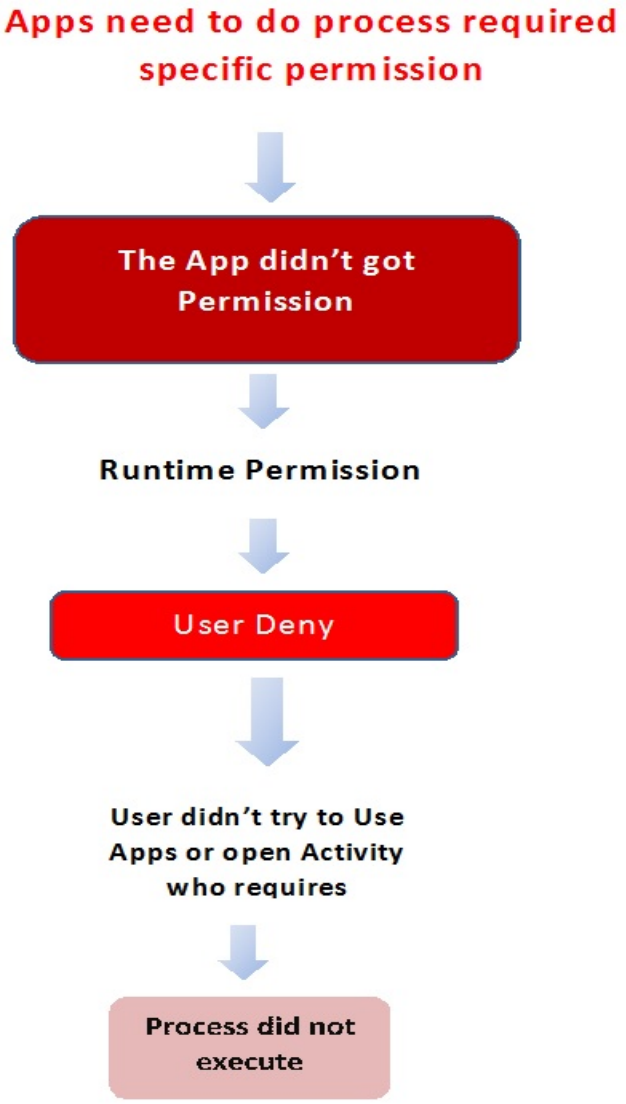
access control in android marshmallow

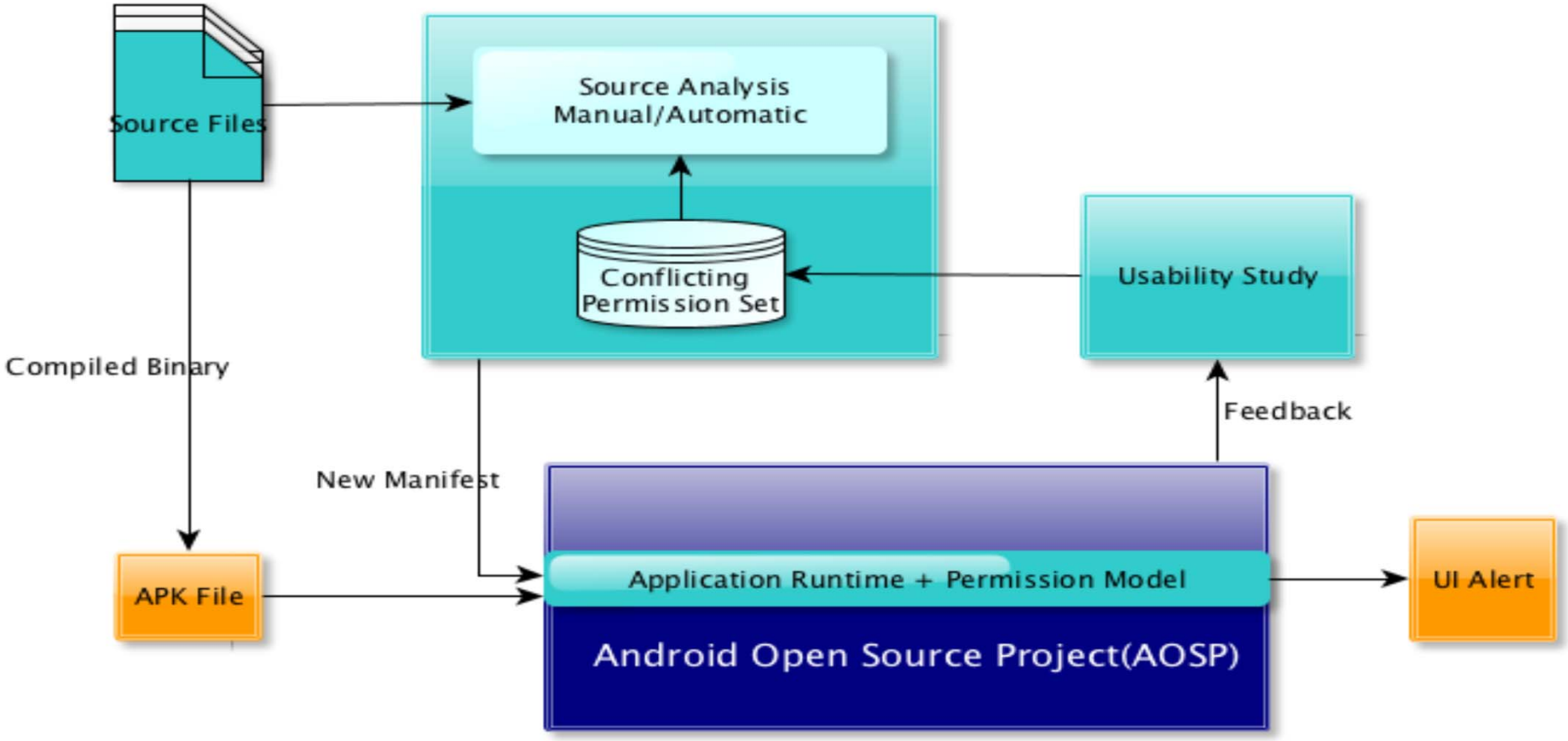
- One of the features in android marshmallow is a permission and it mean
- No need to give apps access all the time. Android Marshmallow lets you define what you want to share and when. Turn permissions off at any time, too.
- The next figure represents the process simply





Now in the new system permission of marshmallow instead of the user accept the permission foe one time before the installation of apps the user will ask for permission any time if the process required that and the user can agree or deny this for making user more secure and add more controlling on apps and this new system for permission apply only with unsecure permissions not in ordinary permission . As you see in the diagram here





Architecture of our Permission Model

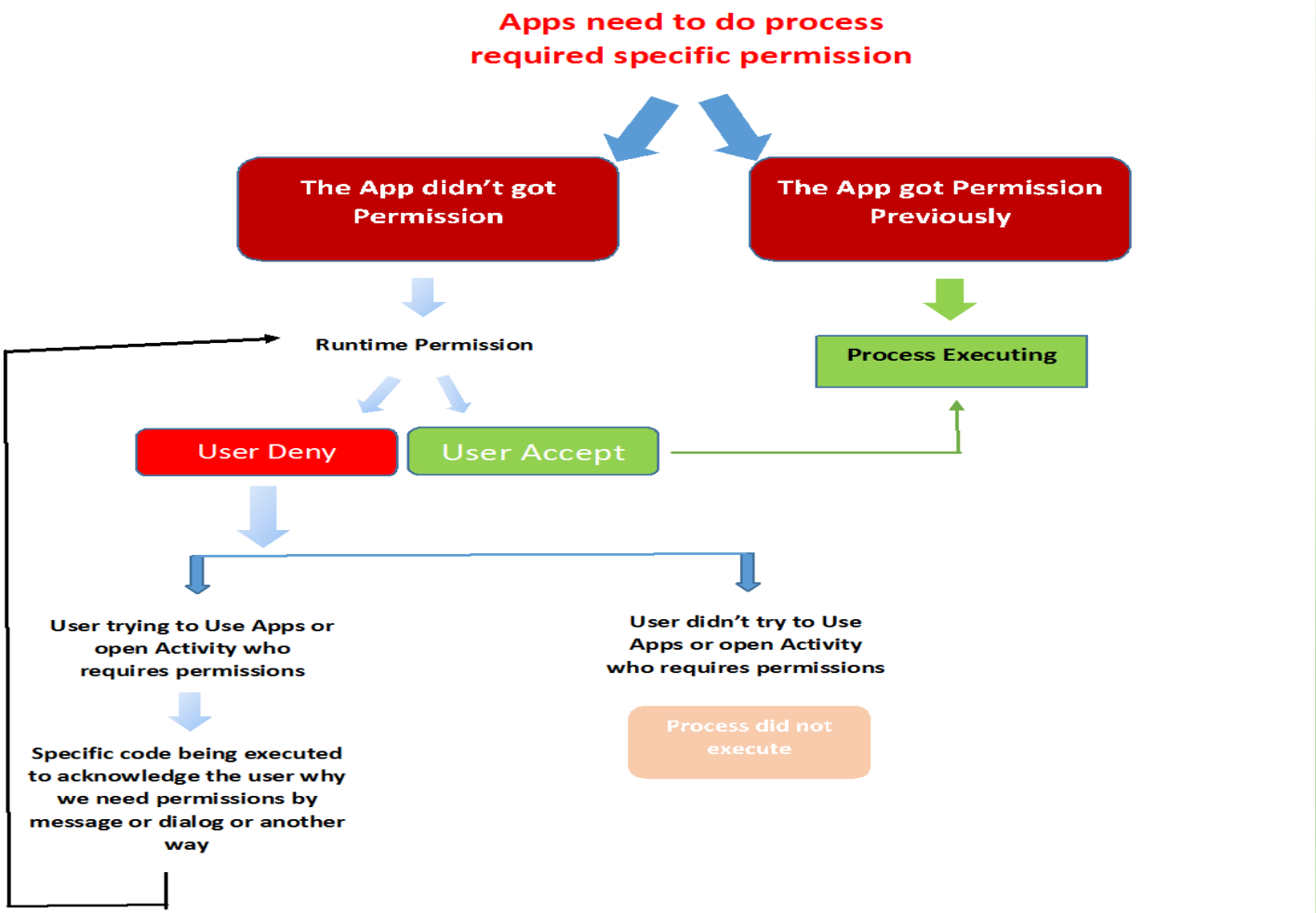
- The access control in Android can be divided into several categories, but the most important are the two categories the first is normal access control are granted approval during the installation of the application There is no risk or contact with the privacy of the user directly such as the ability to connect to the Internet but the second is dangerous access control the application time must be granted by the user And there is a risk to the privacy of the user, for example read the contacts registered on the user's machine

- The dangerous access control are divided into groups of each group that have access that fall under the same category. For example, the access to read the contacts and the access to write contacts that fall under the following set of communication and The next following picture explain these sets of dangerous access and what falls under each set of powers

Dangerous Permissions

Permission Group	Permission
android.permission-group.CALENDAR	• android.permission.READ_CALENDAR • android.permission.WRITE_CALENDAR
android.permission-group.CAMERA	• android.permission.CAMERA
android.permission-group.CONTACTS	• android.permission.READ_CONTACTS • android.permission.WRITE_CONTACTS • android.permission.READ_PROFILE • android.permission.WRITE_PROFILE
android.permission-group.LOCATION	• android.permission.ACCESS_FINE_LOCATION • android.permission.ACCESS_COARSE_LOCATION
android.permission-group.MICROPHONE	• android.permission.RECORD_AUDIO
android.permission-group.PHONE	• android.permission.READ_PHONE_STATE • android.permission.CALL_PHONE • android.permission.READ_CALL_LOG • android.permission.WRITE_CALL_LOG • com.android.voicemail.permission.ADD_VOICEMAIL • android.permission.USE_SIP • android.permission.PROCESS_OUTGOING_CALLS
android.permission-group.SENSORS	• android.permission.BODY_SENSORS • android.permission.USE_FINGERPRINT
android.permission-group.SMS	• android.permission.SEND_SMS • android.permission.RECEIVE_SMS • android.permission.READ_SMS • android.permission.RECEIVE_WAP_PUSH • android.permission.RECEIVE_MMS • android.permission.READ_CELL_BROADCASTS
android.permission-group.STORAGE	• android.permission.READ_EXTERNAL_STORAGE • android.permission.WRITE_EXTERNAL_STORAGE

This Diagram shows all access permissions



References:

- Wikipedia Android Marshmallow
- www.theodysseyonline.com
- http://www.hendiware.com
- www.captechconsulting.com