Android6.0以上 动态权限申请

不受重视的原因：
1.国内的大部分设备都是在Android4.4~Android5.1之间。
2.国内厂商对于Rom的自定义参差不齐，大多数集成了自家的安全中心。
3.安全类软件。

采取措施:
1.将targetSdkVersion版本改为23以下，表示该应用未进行新特性适配。
2.代码中进行新特性适配。

一、权限的提醒：
在Android6.0之前，关于应用使用的权限，仅仅是在安装的时候，会显示该应用需要的权限。安装软件即表示接受所有的权限申请，并且在安装之后并不能再关闭某一个权限。
在新版本的权限系统中，不光是在安装的时候提醒用户改应用所需要的权限，并且在使用到某个权限的时候，会动态的弹出提示框，只有在用户确认之后才会赋予该权限。
相比之下，新版本的权限的掌握权更多的落在了用户的手里，使得手机安全性 更加有所保障。
二、权限的声明：
在Android6.0之前， 权限声明都是在AndroidManifest.xml文件中，通过<uses-permission />标签包裹。
示例：

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE”/>
```

在新版本中，不仅需要在AndroidManifest.xml文件中进行声明，还需要在使用到权限的代码出进行动态的权限申请。

主要的API：

- checkSelfPermission();

  参数：权限字符
  作用：检查当前应用是否拥有传入的权限。
  返回值：int类型
  返回值说明：

```java
    /**
     * Permission check result: this is returned by {@link #checkPermission}
     * if the permission has been granted to the given package.
     */
    public static final int PERMISSION_GRANTED = 0;

    /**
     * Permission check result: this is returned by {@link #checkPermission}
     * if the permission has not been granted to the given package.
     */
    public static final int PERMISSION_DENIED = -1;
```

- shouldShowRequestPermissionRationale();

  参数：权限字符
  作用：判断是否需要给出用户请求该权限的原因
  返回值：boolean类型
  返回值说明：当应用进入，第一次调用该函数，返回false。上次拒绝且没有勾选“不再询问”时调用该函数返回true。 当勾选“不再询问”时调用返回false。

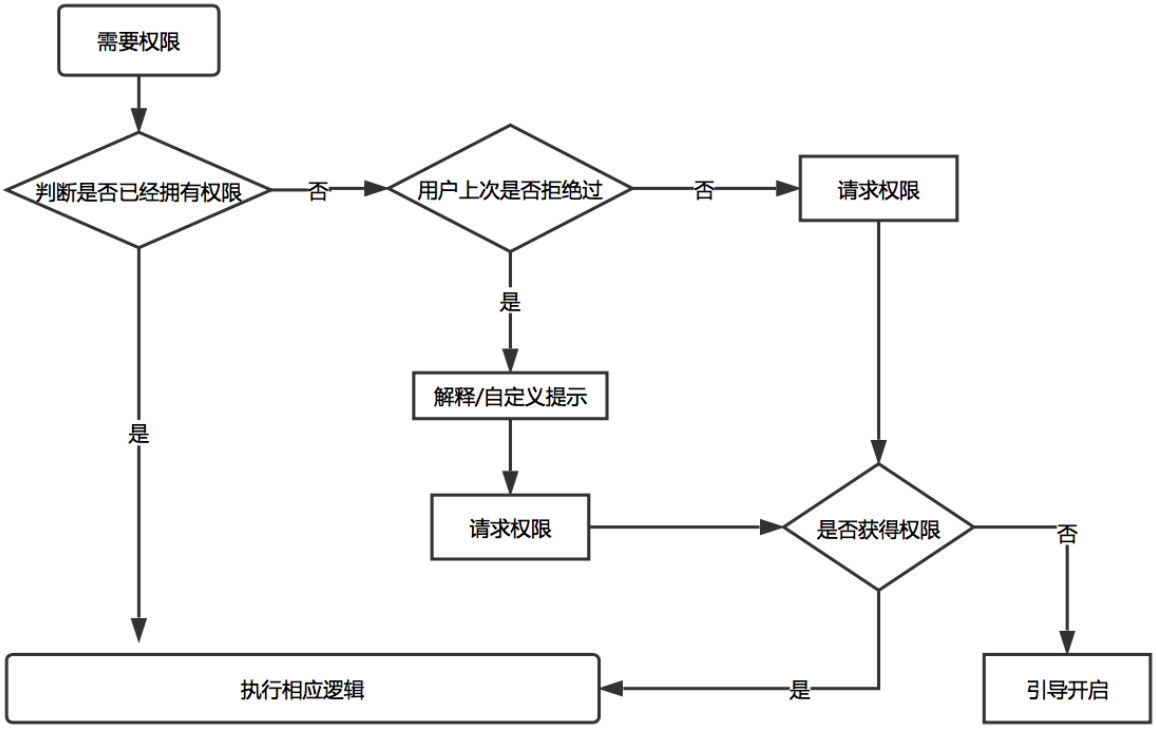
- requestPermissions();

  参数：1️⃣.权限字符串数组 2️⃣.请求码
  作用：请求权限
  返回值：无
  方法说明：请求所需权限，UI界面弹出对应的请求界面。

- 重写onRequestPermissionsResult()方法：

  请求权限结果的回调方法。

一些流程：



三、权限分类：

1.Normal Permission（一般权限）：

- 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

以上这些权限并不会影响用户的手机信息安全，所以只需要在AndroidManifest.xml文件中声明即可。用户无法禁止以上的应用权限。

2.Dangerous Permission（危险权限）

权限组	所有权限
CALENDAR	READ_CALENDAR , WRITE_CALENDAR
CAMERA	CAMERA
CONTACTS	READ_CONTACTS , WRITE_CONTACTS , GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION , ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE , CALL_PHONE , READ_CALL_LOG , WRITE_CALL_LOG , ADD_VOICEMAIL , USE_SIP , PROCESS_OUTGOING_CALLS
SENSORS	BODY_SENSORS
SMS	SEND_SMS , RECEIVE_SMS , READ_SMS , RECEIVE_WAP_PUSH , RECEIVE_MMS
STORAGE	READ_EXTERNAL_STORAGE , WRITE_EXTERNAL_STORAGE

以上权限在读取手机信息，用户存储信息。或者对手机进行读写操作会涉及到用户的隐私，会产生安全问题。所以以上权限在使用的时候，都需要在运行时进行权限申请。注：同一权限组内，其中一个权限通过之后，默认同组内其他权限都是同意的。