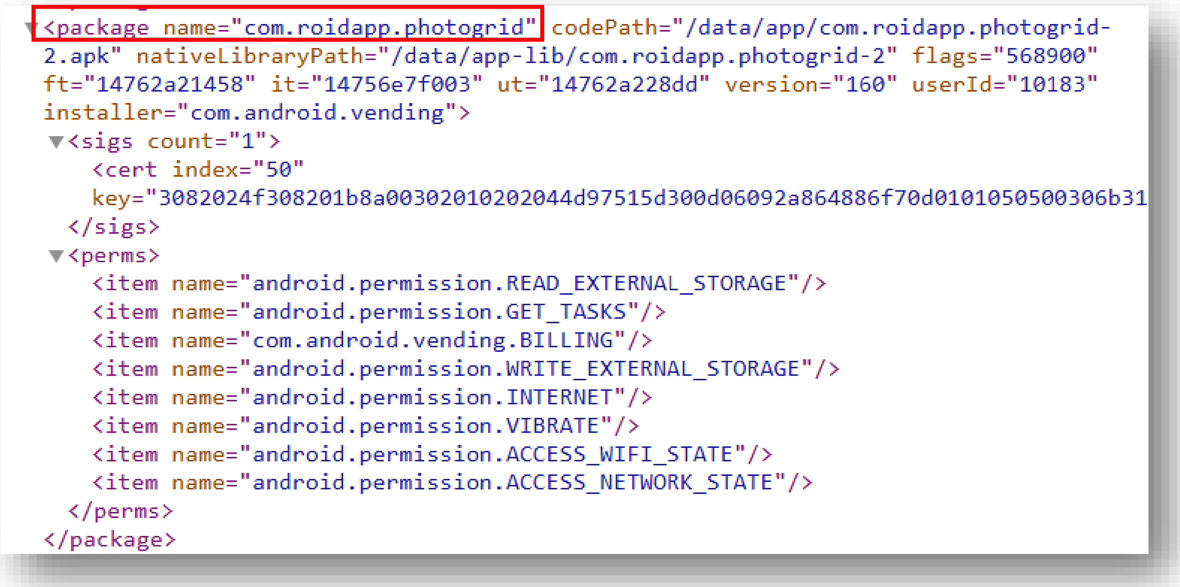
Name: Mohit Ajaykumar Dhabuwala

Assignment: Examination of Packages.xml file from an android phone.

Q1. Examine the Packages.xml file. What are the permissions associated with com.roidapp.photogrid?

Answer: The permissions associated with **"com.roidapp.photogrid"** app which could possibly be a photo editing app named "**photogrid**" are:

- **android.permission.READ_EXTERNAL_STORAGE**: This permission allows the app to read files from the device's external storage, such as the SD card.
- **android.permission.GET_TASKS**: This permission allows the app to retrieve information about currently and recently running tasks.
- **com.android.vending.BILLING**: This permission allows the app to use Google Play's billing service for in-app purchases.
- **android.permission.WRITE_EXTERNAL_STORAGE**: This permission allows the app to write files to the device's external storage.
- **android.permission.INTERNET**: This permission allows the app to access the internet.
- **android.permission.VIBRATE**: This permission allows the app to control the vibrator that provides haptic feedback to the user.
- **android.permission.ACCESS_WIFI_STATE**: This permission allows the app to view information about the state of Wi-Fi, such as whether Wi-Fi is enabled and the name of the connected Wi-Fi network.
- **android.permission.ACCESS_NETWORK_STATE**: This permission allows the app to view information about the state of the network connections, such as whether the device is connected to the internet.



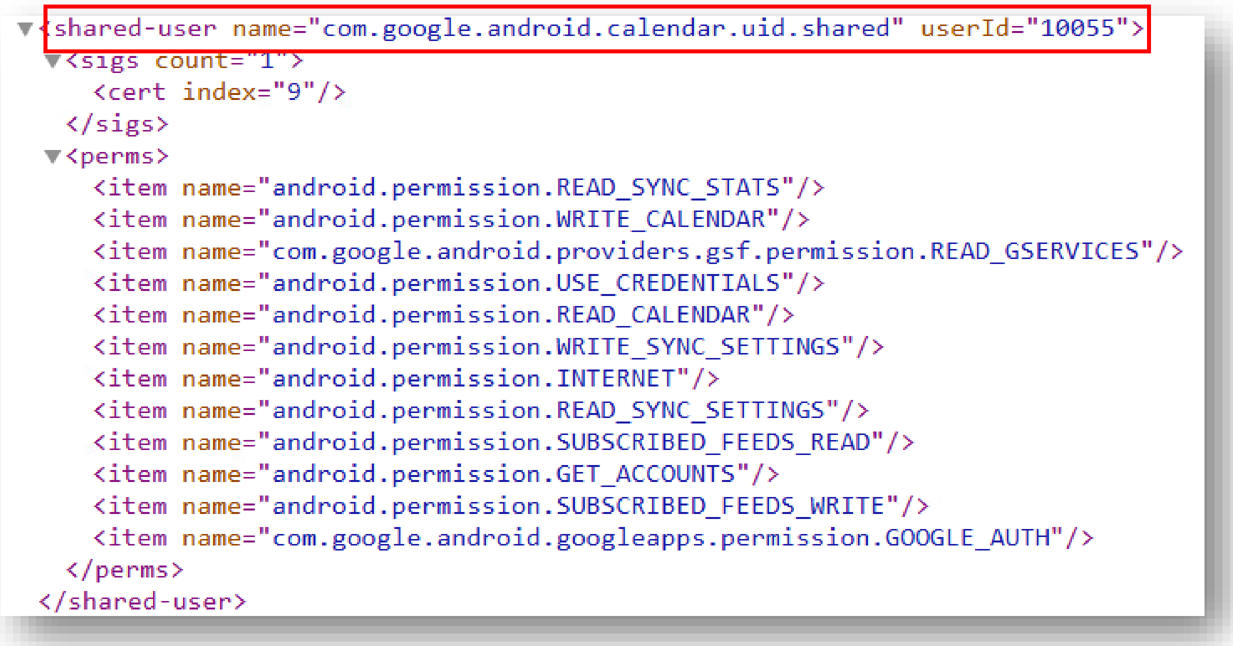
```
▼<package name="com.roidapp.photogrid" codePath="/data/app/com.roidapp.photogrid-
 2.apk" nativeLibraryPath="/data/app-lib/com.roidapp.photogrid-2" flags="568900"
 ft="14762a21458" it="14756e7f003" ut="14762a228dd" version="160" userId="10183"
 installer="com.android.vending">
  ▼<sigs count="1">
     <cert index="50"
     key="3082024f308201b8a00302010202044d97515d300d06092a864886f70d0101050500306b31
   </sigs>
  ▼<perms>
     <item name="android.permission.READ_EXTERNAL_STORAGE"/>
     <item name="android.permission.GET_TASKS"/>
     <item name="com.android.vending.BILLING"/>
     <item name="android.permission.WRITE_EXTERNAL_STORAGE"/>
     <item name="android.permission.INTERNET"/>
     <item name="android.permission.VIBRATE"/>
     <item name="android.permission.ACCESS_WIFI_STATE"/>
     <item name="android.permission.ACCESS_NETWORK_STATE"/>
   </perms>
 </package>
```

Q2. Examine the packagcs.xml file. What permissions would an app have if it accessed com.google.android.calendar.uid.shared (user ID 10055)?

Answer: If an app accessed "**com.google.android.calendar.uid.shared"** (user ID 10055), it would have unrestricted access to the following permissions:

- **android.permission.READ_SYNC_STATS**: The read sync permission allows the app to read the synchronization status for any account on the device. This could include information about when data was last synced, how much data was synced, and whether there were any errors during synchronization.
- **android.permission.WRITE_CALENDAR**: The write permission allows the app to add, edit, and delete events in the user's calendar.
- **com.google.android.providers.gsf.permission.READ_GSERVICES**: Allows the app to read Google service configuration data. This data can include information about the user's Google account, such as their email address and settings.
- **android.permission.USE_CREDENTIALS**: This permission grants the app to request authentication tokens from the associated Account Manager allowing the app to use the credentials stored on the device. This permission is typically used in scenarios where an app needs to access user credentials for authentication purposes, such as logging into a service or accessing secure resources.
- **android.permission.READ_CALENDAR**: This permission allows an app to read and access the user's calendar data, such as events information like the title, description, time, location, and any other relevant metadata about the event stored in the device's calendar app.
- **android.permission.WRITE_SYNC_SETTINGS**: Allows the app to modify the synchronization settings for any account on the device. This could include changing how often data is synced or which data is synced.
- **android.permission.INTERNET**: Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.
- **android.permission.READ_SYNC_SETTINGS**: Allows the app to read the synchronization settings for any account on the device.
- **android.permission.SUBSCRIBED_FEEDS_READ**: Allows the app to get details about the feeds the user is subscribed to such as subscribed calendar feeds or shared calendars.
- **android.permission.GET_ACCOUNTS**: Allows access to the list of accounts in the Accounts Service.
- **android.permission.SUBSCRIBED_FEEDS_WRITE**: Allows an application to modify the feeds the user is subscribed to.

- **com.google.android.googleapps.permission.GOOGLE_AUTH**: This permission allows the app to access the user's Google account and use Google services.



```
<shared-user name="com.google.android.calendar.uid.shared" userId="10055">
  <sigs count="1">
    <cert index="9"/>
  </sigs>
  <perms>
    <item name="android.permission.READ_SYNC_STATS"/>
    <item name="android.permission.WRITE_CALENDAR"/>
    <item name="com.google.android.providers.gsf.permission.READ_GSERVICES"/>
    <item name="android.permission.USE_CREDENTIALS"/>
    <item name="android.permission.READ_CALENDAR"/>
    <item name="android.permission.WRITE_SYNC_SETTINGS"/>
    <item name="android.permission.INTERNET"/>
    <item name="android.permission.READ_SYNC_SETTINGS"/>
    <item name="android.permission.SUBSCRIBED_FEEDS_READ"/>
    <item name="android.permission.GET_ACCOUNTS"/>
    <item name="android.permission.SUBSCRIBED_FEEDS_WRITE"/>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH"/>
  </perms>
</shared-user>
```

A User ID is a unique numerical identifier assigned to each user profile on a device. In this case, the shared user ID 10055 indicates that these permissions are associated with a shared user profile related to the Google Calendar app.

Granting these permissions to Google Calander allows it to access and potentially modify the user's calendar data, including events, attendees, and other critical information. Thus It is advised to be cautious when granting these permissions, especially to any third-party apps, as they could misuse this access and use the user data for any unethical purposes.