Modelo de Permisos en Android

Qué alegría estar juntos de nuevo para seguir conociendo el desarrollo de aplicaciones Android. En esta oportunidad nos centraremos en los permisos requeridos por un usuario al momento de usar nuestra aplicación.

El **propósito de un permiso es proteger la privacidad de un usuario de Android**. Las aplicaciones de Android deben solicitar permiso para acceder a datos confidenciales del usuario (como contactos y SMS), así como a ciertas funciones del sistema (como cámara e Internet). Dependiendo de la función, el sistema puede otorgar el permiso automáticamente o puede solicitar al usuario que apruebe la solicitud.

Un punto de diseño central de la arquitectura de seguridad de Android es **que ninguna aplicación, por defecto, tiene permiso para realizar operaciones que impacten negativamente a otras aplicaciones**, al sistema operativo o al usuario. Esto incluye leer o escribir los datos privados del usuario (como contactos o correos electrónicos), leer o escribir los archivos de otra aplicación, acceder a la red, mantener el dispositivo despierto, entre otros.

Aprobación del permiso

Una aplicación debe publicitar los permisos que requiere mediante la inclusión de etiquetas `<uses-permission>` en el manifiesto de la aplicación. Por ejemplo, una aplicación que necesita enviar mensajes SMS tendría esta línea en el manifiesto:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
 package="com.nextu.miapp">
 <uses-permission android:name="android.permission.SEND_SMS"/>
 <application ...>
 ...
 </application> </manifest>
```

Si nuestra aplicación enumera los permisos normales en su manifiesto (es decir, permisos que no representan un gran riesgo para la privacidad del usuario o el funcionamiento del dispositivo), el sistema otorga automáticamente esos permisos a nuestra aplicación.

Si nuestra aplicación enumera permisos peligrosos en su manifiesto (es decir, permisos que podrían afectar la privacidad del usuario o el funcionamiento normal del dispositivo), como el permiso SEND_SMS anterior, el usuario debe aceptar explícitamente otorgar esos permisos.

Solicitar permisos peligrosos

Sólo los permisos peligrosos requieren un acuerdo del usuario. La forma en que Android le pide al usuario que otorgue permisos peligrosos depende de la versión de

Android que se ejecuta en el dispositivo del usuario y de la versión del sistema a la que apunta tu aplicación.

Solicitar permisos para acceder a información confidencial del usuario

Algunas aplicaciones dependen del acceso a información confidencial del usuario relacionada con registros de llamadas y mensajes SMS. Si deseamos **solicitar los permisos específicos para registros de llamadas y mensajes SMS**, además de publicar nuestra aplicación en Play Store, **debemos solicitar al usuario que configure nuestra aplicación como el controlador predeterminado** (default handler) para una función central del sistema, antes de solicitar estos permisos de tiempo de ejecución.

Permisos para funciones de hardware opcionales

El acceso a algunas funciones de hardware (como Bluetooth o la cámara) requieren un permiso de aplicación. Sin embargo, no todos los dispositivos Android tienen estas características de hardware. Entonces, si tu aplicación solicita el permiso CÁMARA, es importante que también incluya la etiqueta ><uses-feature> en su manifiesto para declarar si esta característica es realmente necesaria o no. Por ejemplo:

```
<uses-feature android: name = "android.hardware.camera" android: required
= "false" />
```

Si declara android: required = "false" para la función, Google Play permite que nuestra aplicación se instale en dispositivos que no tienen la característica. Luego debemos verificar si el dispositivo actual tiene la característica en tiempo de ejecución, llamando a PackageManager.hasSystemFeature () y deshabilitarla “elegantemente” si no está disponible.

Si no se proporciona la etiqueta <uses-feature>, cuando Google Play vea que nuestra aplicación solicita el permiso correspondiente, asume que requiere esta función. Por lo tanto, filtra nuestra aplicación para los dispositivos sin la función, como si se declarara android: required = "true" en la etiqueta<uses-feature>.

Niveles de protección

Los permisos se dividen en varios niveles de protección. El nivel de protección afecta si se requieren solicitudes de permiso en tiempo de ejecución. **Hay tres niveles de protección** que afectan las aplicaciones de terceros: **permisos normales, de firma y peligrosos**.

Permisos normales

Los permisos normales cubren áreas donde nuestra aplicación necesita acceder a datos o recursos fuera del entorno limitado de la aplicación, pero donde hay muy poco riesgo para la privacidad del usuario o el funcionamiento de otras aplicaciones. Por ejemplo, el permiso para establecer la zona horaria es un permiso normal.

Si una aplicación declara en su manifiesto que necesita un permiso normal, el sistema otorga automáticamente ese permiso a la aplicación en el momento de la instalación. El sistema no solicita al usuario que otorgue permisos normales y los usuarios no pueden revocar estos permisos.

Permisos de firma

El sistema otorga estos permisos de aplicación en el momento de la instalación, pero sólo cuando la aplicación, que intenta usar un permiso, está firmada por el mismo certificado que la aplicación que define el permiso.

Permisos peligrosos

Los permisos peligrosos cubren áreas donde la aplicación quiere datos o recursos que involucren la información privada del usuario, o que puedan afectar los datos almacenados del usuario o el funcionamiento de otras aplicaciones. Por ejemplo, la capacidad de leer los contactos del usuario es un permiso peligroso. Si una aplicación declara que necesita un permiso peligroso, el usuario debe otorgar explícitamente el permiso a la aplicación. Hasta que el usuario apruebe el permiso, tu aplicación no puede proporcionar funciones que dependan de ese permiso.

Para usar un permiso peligroso, tu aplicación debe solicitar al usuario que otorgue el permiso en tiempo de ejecución.

Permisos especiales

Hay un par de permisos que no se comportan como permisos normales y peligrosos. **SYSTEM_ALERT_WINDOW y WRITE_SETTINGS son particularmente sensibles**, por lo que la mayoría de las aplicaciones no deberían usarlos. Si una aplicación necesita uno de estos permisos, debe declarar el permiso en el manifiesto y enviar un intent solicitando la autorización del usuario. El sistema responde al intent mostrando una pantalla de administración detallada al usuario.

Grupos de permisos

Los permisos se organizan en grupos relacionados con las capacidades o características de un dispositivo. Bajo este sistema, las solicitudes de permisos se manejan a nivel de grupo y un solo grupo de permisos corresponde a varias declaraciones de permisos en el manifiesto de la aplicación. Por ejemplo, **el grupo de SMS incluye las**

declaraciones READ_SMS y RECEIVE_SMS. La agrupación de permisos de esta manera permite al usuario tomar decisiones más significativas e informadas, sin verse abrumado por solicitudes de permisos complejos y técnicos.

Todos los permisos peligrosos de Android pertenecen a grupos de permisos. Cualquier permiso puede pertenecer a un grupo de permisos independientemente del nivel de protección. Sin embargo, un grupo de permisos sólo afecta la experiencia del usuario, si el permiso es peligroso.

Hemos finalizado este rincón didáctico y esperamos verte pronto nuevamente.