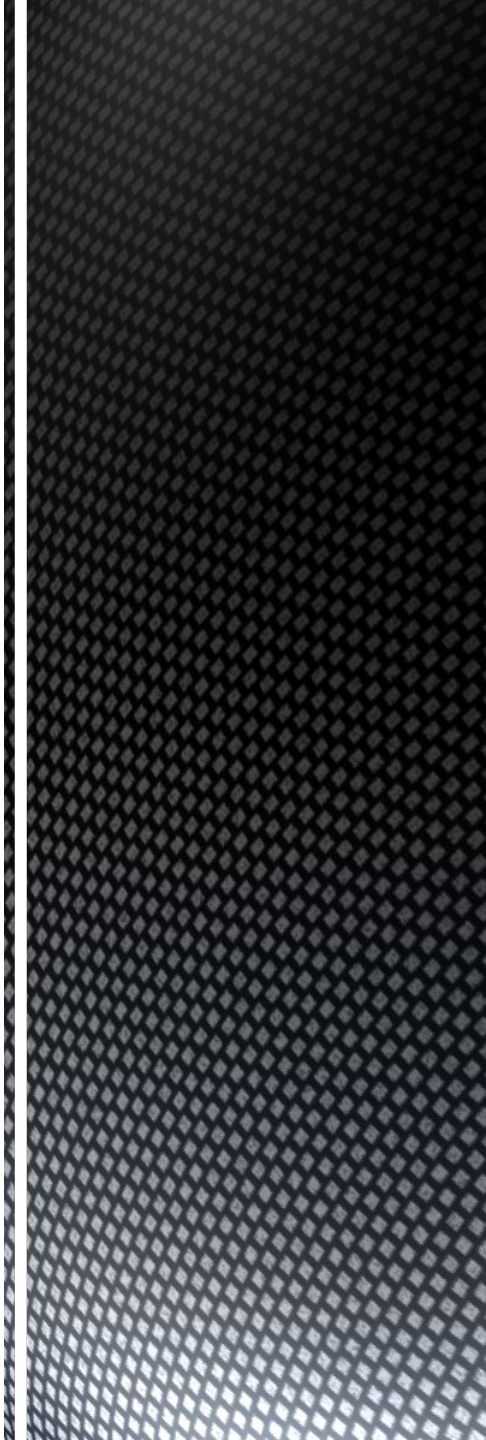
Permisos



Seguridad en Android

La seguridad en Android se basa en:

- Seguridad de Linux.

  Android puede impedir que las aplicaciones tengan acceso directo al hardware o interfieran con recursos de otras aplicaciones.

- Toda aplicación ha de ser firmada con un certificado digital que identifique a su autor.

  La firma digital también nos garantiza que el fichero de la aplicación no ha sido modificado.

  Si se desea modificar la aplicación está tendrá que ser firmada de nuevo, y esto solo podrá hacerlo el propietario de la clave privada.

  Es habitual que un certificado digital sea firmado a su vez por una autoridad de certificación, sin embargo en Android esto no es necesario.

- Mediante un modelo de permisos facilitamos el acceso a partes y funcionalidades del sistema. El usuario deberá aprobar el uso de esos permisos y asumir los riesgos que conllevan.

Permisos

Android usa los permisos para proteger:

- Recursos,
- Información y
- Operaciones.

Las aplicaciones también pueden definir y forzar sus propios permisos con el fin de limitar el acceso a recursos e información del usuario.

Ejemplos:

Restringir quien tiene acceso a la Base de Datos de la aplicación

Restringir el acceso a operaciones con coste (SMS, MMS)

Restringir acceso a recursos como el uso de la cámara

En Android los permisos se representan como una cadena de caracteres (String)

Las aplicaciones declaran estos permisos en el AndroidManifest.xml:

- **Los permisos que nuestra aplicación usará** (necesita) nuestra aplicación
- **Los permisos que nuestra aplicación exige** a otros componentes para que la usen.

Permisos

Cuando una aplicacion necesita usar un permiso lo declara con la etiqueta xml <uses-permission>.

De esta manera cuando la aplicación se instala en un dispositivo el usuario tendrá que aceptar que dicha aplicación acceda a ese permiso.

```
<manifest … >
   <uses-permission android:name="android.permission.CAMERA”/>
   <uses-permission android:name="android.permission.INTERNET”/>
   <uses-permission android:name=“android.permission.ACCESS_FINE_LOCATION”/>
</manifest >
```

Los Strings que identifican los permisos están declarados en la clase Manifest.permission

- Si la aplicación lista permisos normales (que no ponen en riesgo la privacidad del usuario o la operativa del dispositivo), **Android automáticamente otorga estos permisos**.
- Si la aplicación lista permisos peligrosos **Android pregunta al usuario**
  - A partir de la versión 6.0 (API level 23) la consulta se realiza en tiempo de ejecución, una vez o cada vez que corra.
  - Si corre la versión 5.1 (API level 22) o inferior la consulta se realiza en tiempo de instalación. Una vez instalada y aprobados para revocar hay que desinstalar.

Permisos

Group Permissions

A partir de la versión 6.0 (API 23) el comportamiento cuando se pide un dangerous permission depende de lo siguiente

- Si la App **no tiene** permisos del grupo al que pertenece el dangerous permission entonces pide el permiso explícitamente al usuario
- Si la App **tiene** permisos del mismo grupo, ya otorgados por el usuario, Android otorga el permiso directamente sin preguntar al usuario.

Permissions Android Developers

Runtime Permissions

Categorías de Permisos

Grupos de Permisos Peligrosos

- Almacenamiento Externo
- Ubicación
- Teléfono
- Mensajes de texto (SMS)
- Contactos
- Calendario
- Cámara
- Micrófono
- Sensores Corporales

Categorías Permisos Normales

- Comunicaciones
- Conexión Wifi
- Bluetooth
- Consumo Batería
- Aplicaciones
- Configuraciones del Sistema
- Audio
- Sincronización
- Ubicación
- Seguridad

Permisos Peligrosos

- Almacenamiento Externo
  - WRITE_EXTERNAL_STORAGE– Modificar/eliminar almacenamiento USB (API 4). Permite el borrado y la modificación de archivos en la memoria externa. Lo ha de solicitar toda aplicación que necesite escribir un fichero en la memoria externa; por ejemplo, exportar datos en XML. Pero al permitirlo también podrán modificar/eliminar ficheros externos creados por otras aplicaciones.
  - READ_EXTERNAL_STORAGE– Leer almacenamiento USB (API 16). Permite leer archivos en la memoria externa. Este permiso se ha introducido en la versión 4.1. En versiones anteriores todas las aplicaciones pueden leer en la memoria externa. Por lo tanto, has de tener cuidado con la información que dejas en ella.

Permisos Peligrosos

- Ubicación
  - ACCESS_COARSE_LOCATION –Localización no detallada (basada en red). Localización basada en telefonía móvil (*Cell-ID*) y Wi-Fi. Aunque en la actualidad esta tecnología suele ofrecernos menos precisión que el GPS, no siempre es así. Por ejemplo, se está aplicando en el interior de aeropuertos y museos con precisiones similares.
  - ACCESS_FINE_LOCATION –Localización GPS detallada. Localización basada en satélites GPS. Al dar este permiso también estamos permitiendo la localización basada en telefonía móvil y Wi-Fi (ACCESS_COARSE_LOCATION).

Permisos Peligrosos

- Teléfono
  - CALL_PHONE –Llamar a números de teléfono directamente **Servicios por los que tienes que pagar**. Permite realizar llamadas sin la intervención del usuario. Nunca solicites este permiso en tus aplicaciones, muchos usuarios no instalarán tu aplicación. Si has de realizar una llamada, es mejor realizarla por medio de una intención. A diferencia de la llamada directa, no necesitas ningún permiso, dado que el usuario ha de pulsar el botón de llamada para que comience.
  - READ_PHONE_STATE –Consultar identidady estado del teléfono.. Muchas aplicaciones, como los juegos, piden este permiso para ponerse en pausa cuando recibes una llamada. Sin embargo, también permite el acceso al número de teléfono, IMEI (identificador de teléfono GSM), IMSI (identificador de tarjeta SIM) y al identificador único de 64 bits que Google asigna a cada terminal. Incluso si hay una llamada activa, podemos conocer el número al que se conecta la llamada.
  - READ_CALL_LOG y WRITE_CALL_LOG –Leer y modificar el registro de llamadas telefónicas. Como realizar estas acciones se describe al final del capítulo 9.
  - ADD_VOICEMAIL –Añadir mensajes de voz. Permite crear nuevos mensajes de voz en el sistema.
  - USE_SIP –Usar Session Initial Protocol. (API 9). Permite a tu aplicación usar el protocolo SIP.
  - PROCESS_OUTGOING_CALLS –Procesar llamadas salientes. Permite a la aplicación controlar, modificar o abortar las llamadas salientes.

Permisos Peligrosos

- Mensajes de texto (SMS)
  - SEND_SMS –Enviar mensaje SMS **Servicios por los que tienes que pagar**. Permite la aplicación mandar de texto SMS sin la validación del usuario. Por iguales razones que CALL_PHONE, a no ser que tu aplicación tenga que mandar SMS sin la intervención del usuario, resulta más conveniente enviarlos por medio de una intención.
  - RECEIVE_SMS –Recibir mensajes de texto. Permite a la aplicación recibir y procesar SMS. Una aplicación puede modificar o borrar los mensajes recibidos
  - READ_SMS –Leer mensajes de texto. Permite a la aplicación leer los mensajes SMS entrentes.
  - RECEIVE_MMS – Recibir mensajes MMS. Permite monitorizar los mensajes multimedia entrantes, pudiendo acceder a su contenido.
  - RECEIVE_WAP_PUSCH – Recibir mensajes WAP Push. Permite monitorizar los mensajes WAP Push entrantes. Un mensaje WAP PUSH es un tipo de SMS que se usa para acceder de manera sencilla a una página WAP en lugar de teclear su direccion URL en el navegador.

Permisos Peligrosos

- Contactos
- READ_CONTACTS – Leer datos de contactos. Permite leer información sobre los contactos almacenados (nombres, correos electrónicos, números de teléfono). Algunas aplicaciones podrían utilizar esta información de forma no lícita
- WRITE_CONTACTS – Escribir datos de contactos. Permite modificar los contactos.
- GET_ACCOUNTS – Obtener Cuentas. Permiten acceder a la lista de cuentas en el Servicio de Cuentas[1].

Permisos Peligrosos

- Calendario
  - READ_CALENDAR – Leer datos de contactos. Permite leer información del calendario del usuario.
  - WRITE_CONTACTS – Escribir datos de contactos. Permite escribir en el calendario, pero no leerlo.
- Cámara
  - CAMARA – Hacer fotos / grabar vídeos. Permite acceso al control de la cámara y a la toma de imágenes y vídeos. El usuario puede no ser consciente.
- Micrófono
  - RECORD_AUDIO – Grabar audio. Permite acceso grabar sonido desde el micrófono del teléfono.
- Sensores Corporales
  - BODY SENSORS – Leer sensores corporales. Da acceso a los datos de los sensores que están monitorizando el cuerpo del usuario. Por ejemplo, el lector de ritmo cardiaco.

Permisos Normales

- Comunicaciones
  - INTERNET – Acceso a Internet sin límites. Permite establecer conexiones a través de Internet. Este es un permiso muy importante, en el que hay que fijarse a quién se otorga.La mayoría de las aplicaciones lo piden, pero no todas lo necesitan.
    Cualquier *malware* necesita una conexión para poder enviar datos de nuestro dispositivo.
  - ACCESS_NETWORK_STATE –Ver estado de red. Información sobre todas las redes. Por ejemplo para saber si tenemos conexión a internet.
  - CHANGE_NETWORK_STATE – Cambiar estado de red. Permite cambiar el estado de conectividad de redes.
  - NFC – Near field communication. (API 19) Algunos dispositivos disponen de un trasmisor infrarrojo para el control remoto de electrodomésticos.
  - TRASMIT_R – Trasmitir por infrarrojos. (API 19) Algunos dispositivos disponen de un trasmisor infrarrojo para el control remoto de electrodomésticos.

Permisos Normales

- Conexión Wifi
  - ACCESS_WIFI_STATE – Ver estado de Wi-Fi. Permite conocer las redes Wi-Fi disponibles.
  - CHANGE_WIFI_STATE – Cambiar estado de Wi-Fi. Permite cambiar el estado de conectividad Wi-Fi.
  - CHANGE_WIFI_MULTICAST_STATE – Cambiar estado multicast Wi-Fi (API 4). Permite pasar al modo Wi-Fi Multicast.
- Bluetooth
  - BLUETOOTH – Crear conexión Bluetooth. Permite a una aplicación conectarse con otro dispositivo Bluetooth. Antes ambos dispositivos han de emparejarse
  - .BLUETOOTH_ADMIN – Emparejar Bluetooth. Permite descubrir y emparejarse con otros dispositivos Bluetooth.
- Consumo Batería
  - WAKE_LOCK –Impedir que el teléfono entre en modo de suspensión. Para algunas aplicaciones, como un navegador GPS, puede ser importante que no sean suspendidas nuca. Realmente, a lo único que puede afectar es a nuestra batería.
  - FLASHLIGHT – Linterna. Permite encender el flash de la cámara.
  - VIBRATE – Control de la vibración. Permite hacer vibrar al teléfono. Los juegos suelen utilizarlo.

Permisos Normales

- Aplicaciones
  - RECEIVE_BOOT_COMPLETED – Ejecución automática al encender el teléfono. Permite a una aplicación recibir el anuncio broadcast ACTION_BOOT_COMPLETED enviado cuando el sistema finaliza un inicio. Gracias a esto la aplicación pondrá ponerse en ejecución al arrancar el teléfono.
  - BROADCAST_STICKY – Enviar anuncios broadcast permanentes. Un broadcast permanente llegará a los receptores de anuncios que actualmente estén escuchando, pero también a los que se instancien en un futuro. Por ejemplo, el sistema emite el anuncio broadcast ACTION_BATTERY_CHANGED de forma permanente. De esta forma, cuando se llama a registerReceiver() se obtiene la intención de la última emisión de este anuncio. Por lo tanto, puede usarse para encontrar el estado de la batería sin necesidad de esperar a un futuro cambio en su estado. Se ha incluido este permiso dado que las aplicaciones mal intencionadas pueden ralentizar el dispositivo o volverlo inestable al demandar demasiada memoria.
  - KILL_BACKGROUND_PROCESSES – Matar procesos en Background(API 9). Permite llamar a killBackgroundProcesses(String). Al hacer esta llamada el sistema mata de inmediato a todos los procesos de fondo asociados con el paquete indicado. Es el mismo método que usa el sistema cuando necesita memoria. Estos procesos serán reiniciados en el futuro, cuando sea necesario.
  - REORDER_TASKS – Reordenar tareas. Permite a una aplicación cambiar el orden de la lista de tareas.
  - INSTALL_SHORTCUT y UNINSTALL_SHORTCUT– Instalar y desinstalar acceso directo(API 19). Permite a una aplicación añadir o eliminar un acceso directo a nuestra aplicación en el escritorio.
  - GET_PACKAGE_SIZE – Obtener tamaño de un paquete. Permite a una aplicación conocer el tamaño de cualquier paquete.
  - EXPAND_STATUS_BAR – Expandir barra de estado. Permite a una aplicación expandir o contraer la barra de estado

Permisos Normales

- Configuraciones del Sistema
  - CHANGE_CONFIGURATION – Modificar la configuración global del sistema. Permite cambiar la configuración del sistema (como la configuración local)
  - SET_WALLPAPER – Poner fondo de pantalla. Permite establecer fondo de pantalla en el escritorio.
  - SET_WALLPAPER_HITS – Sugerencias de fondo de pantalla. Permite a las aplicaciones establecer sugerencias de fondo de pantalla.
  - SET_ALARM – Establecer Alarma. Permite a la aplicación enviar una intención para poner una alarma o temporizador en la aplicación Reloj.
  - SET_TIME_ZONE – Cambiar zona horario. Permite cambiar la zona horaria del sistema.
  - ACCESS_NOTIFICATION_POLICY – Acceso a política de notificaciones (API 23). Permite conocer la política de notificaciones del sistema.
- Audio
  - MODY_AUDIO_SETTINGS– Cambiar ajustes de audio. Permite cambiar ajustes globales de audio, como el volumen.
- Sincronización
  - READ_SYNC_SETTINGS – Leer ajustes de sincronización. Permite saber si tienes sincronización en segundo plano con alguna aplicación (como con un cliente de Twitter o Gmail).
  - WRITE_SYNC_SETTINGS – Escribir ajustes de sincronización. Permite registrar tu aplicación como adaptador de sincronización (SyncAdapter).
  - READ_SYNC_STATS – Leer estadísticas de sincronización.

Permisos Normales

- Ubicación
  - ACCESS_LOCATION_EXTRA_COMMANDS – Mandar comandos extras de localización. Permite a una aplicación acceder a comandos adicionales de los proveedores de localización. Por ejemplo, tras pedir este permiso podríamos enviar el siguiente comando al GPS, con el método: sendExtraCommand("gps", "delete_aiding_data", null);.
- Seguridad
  - USE_FINGERPRINT– Usar huella digital(API 23). Permite usar el hardware de reconocimiento de huella digital.
  - DISABLE_KEYGUARD – Deshabilitar bloqueo de teclado. Permite a las aplicaciones desactivar el bloqueo del teclado si no es seguro.