UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA

Application Permissions

PRESENTADO POR

Perez Bello Vanory Esperanza

GRUPO

10° B

MATERIA

Desarrollo movil Integral

PROFESOR

Ray Brunett Parra Galaviz

Tijuana, Baja California, 24 Enero del 2025

Application Permissions

Las permisos de aplicaciones son una característica clave en los sistemas operativos móviles, como Android e iOS, que controlan el acceso a recursos y funciones específicas del dispositivo. Los permisos permiten a las aplicaciones interactuar con recursos del sistema, como la cámara, la ubicación, el almacenamiento o los contactos, mientras que aseguran la privacidad y seguridad del usuario.

Tipos de permisos de aplicaciones:

1. **Permisos de acceso a datos del dispositivo:**
    - **Ubicación (GPS):** Permite a las aplicaciones acceder a la ubicación geográfica del dispositivo, lo que es útil para aplicaciones de mapas, navegación o servicios basados en ubicación.
    - **Contactos:** Accede a los contactos guardados en el dispositivo para ofrecer funciones como la mensajería o la sincronización con redes sociales.
    - **Calendario:** Permite a la aplicación leer y modificar los eventos del calendario del dispositivo, lo que se utiliza en aplicaciones de planificación y recordatorios.
    - **Cámara:** Accede a la cámara del dispositivo para capturar fotos o grabar videos, utilizado por aplicaciones como redes sociales, mensajería o escáneres de códigos QR.
    - **Micrófono:** Permite la grabación de audio para funciones como la grabación de notas de voz o llamadas de voz en aplicaciones de mensajería o videoconferencia.

2. **Permisos de acceso a almacenamiento:**
    - **Almacenamiento interno/externo:** Permite que las aplicaciones lean y escriban en el almacenamiento del dispositivo, útil para guardar fotos, archivos y otros datos de la aplicación.

- **Archivos multimedia (fotos, videos, música):** Da acceso a los archivos multimedia almacenados en el dispositivo para ver o modificar contenido dentro de la aplicación.

3. **Permisos de acceso a servicios del sistema:**
    - **Redes y conexiones:** Accede a la información de la red (Wi-Fi, datos móviles) para gestionar la conectividad o realizar transferencias de datos.
    - **Bluetooth:** Permite a la aplicación interactuar con dispositivos Bluetooth cercanos, utilizado en aplicaciones de dispositivos IoT, transferencia de archivos o conexión a dispositivos como audífonos o relojes inteligentes.
    - **Vibración y notificaciones:** Permite a la aplicación controlar las notificaciones del dispositivo, incluyendo la vibración y la emisión de sonidos.

4. **Permisos avanzados:**
    - **Acceso a cámaras frontales, sensores biométricos (huella digital, reconocimiento facial):** Usado por aplicaciones que requieren autenticación biométrica para iniciar sesión o realizar pagos.
    - **Acceso a la ubicación precisa:** Algunas aplicaciones requieren acceso continuo a la ubicación precisa, lo que se utiliza en aplicaciones de transporte o rastreo.

Control de permisos en Android e iOS:

1. **Android:**
    - En **Android**, los permisos se dividen en dos tipos: **normales** y **sensibles**. Los permisos normales son concedidos automáticamente, como el acceso a la red Wi-Fi, mientras que los permisos sensibles requieren la aprobación explícita del usuario, como el acceso a la ubicación o la cámara.

- Con **Android 6.0 (Marshmallow)** y versiones posteriores, el sistema implementó un modelo de permisos **en tiempo de ejecución**, lo que significa que la aplicación solicita los permisos cuando realmente los necesita, en lugar de pedir todos los permisos al instalar la app. Esto da a los usuarios un control más granular sobre los permisos que otorgan.

2. **iOS:**
    - En **iOS**, Apple también requiere que las aplicaciones soliciten permisos para acceder a ciertos recursos. La interfaz del sistema es más estricta en cuanto a la visibilidad de los permisos solicitados y proporciona alertas claras sobre el tipo de datos que la aplicación desea utilizar.
    - **iOS 14** introdujo un cambio significativo al permitir a los usuarios otorgar permisos de forma más específica, como el acceso a la ubicación aproximada en lugar de la ubicación precisa, y mostrar a los usuarios una lista de las aplicaciones que han accedido a sus datos.

Beneficios de los permisos:

- **Protección de la privacidad:** Los permisos limitan el acceso a datos sensibles y recursos del dispositivo, lo que protege la privacidad del usuario. Esto es crucial especialmente en un contexto donde los usuarios son más conscientes de cómo se utilizan sus datos personales.
- **Control del usuario:** Los sistemas operativos modernos permiten a los usuarios gestionar y revisar los permisos en cualquier momento, lo que ofrece un control más directo sobre qué aplicaciones pueden acceder a qué información.
- **Seguridad:** Los permisos también ayudan a mitigar los riesgos de seguridad, limitando el acceso a partes críticas del dispositivo, como el micrófono o la cámara, evitando posibles vulnerabilidades o accesos no deseados.

Desafíos y mejores prácticas:

- **Solicitar permisos con claridad:** Las aplicaciones deben solicitar permisos de manera clara y específica, explicando por qué necesitan el acceso y qué funciones ofrecerán a cambio. Las solicitudes de permisos confusas o invasivas pueden generar desconfianza en los usuarios.
- **Evitar la sobrecarga de permisos:** Las aplicaciones deben solicitar solo los permisos que realmente necesitan para funcionar. Solicitar permisos innecesarios puede aumentar la tasa de rechazo de la aplicación por parte de los usuarios.
- **Respetar la decisión del usuario:** Si un usuario rechaza un permiso, la aplicación debe ser capaz de funcionar correctamente sin ese permiso, proporcionando una experiencia de usuario sin fricciones. En algunos casos, es útil ofrecer funcionalidades alternativas que no dependan del permiso rechazado.

Casos comunes de mal uso de permisos:

- **Acceso innecesario a datos:** Algunas aplicaciones han sido criticadas por solicitar permisos que no son relevantes para sus funcionalidades principales, como acceder a los contactos o la ubicación sin razón justificada.
- **Permisos ocultos:** En algunos casos, las aplicaciones solicitan permisos de forma encubierta o de manera que los usuarios no pueden fácilmente entender qué datos se están accediendo.

Conclusión:

Los **permisos de aplicaciones** son fundamentales para la seguridad y privacidad en los dispositivos móviles. Tanto desarrolladores como usuarios deben ser conscientes de los permisos que se solicitan y de cómo pueden afectar la experiencia general. Un uso responsable de los permisos asegura que las aplicaciones ofrezcan sus funcionalidades sin comprometer la privacidad o seguridad del usuario.