CySec News

2019 AGOSTO

PERMISOS EN APLICACIONES ANDROID

INTRODUCCIÓN

Recordemos que hace unos años atrás cuando instalábamos una apk en nuestro móvil Android las aplicaciones solicitaba una serie de permisos, la lista podía ser entre 4 a 14 permisos en promedio dependiendo de la aplicación que se esté instalando; así el usuario podía decidir otorgarlas o no, si se le negaba la aplicación se detenía o no funcionaba correctamente, dense cuenta de que hoy en día, no pasa eso; ¿Por qué? Para no agobiar a los usuarios con una enorme lista de permisos se resolvió en que los mismos se solicitarán en otro momento cuando corra la aplicación y el usuario llame al recurso a través de esta.

SOBRE LOS PERMISOS

Los permisos para la aplicación Android se declaran desde las etiquetas **Android permission** en el archivo manifest.xml, mas donde se hace el llamado, en el código antes de ejecutar la función que utiliza dicho recurso y en donde se verifica si el equipo tiene el recurso activo de lo contrario el usuario deberá de activarlo.

Si el usuario no otorga el permiso, hay aplicaciones que mediante código pueden saltarse dicha excepción u otras insistir con un mensaje de que se activen. Desde que las aplicaciones apuntan a Android Marshmallow, [fuente developer.android.com]; los permisos se solicitan durante la ejecución (Runtime permissions) y ya no durante la instalación como antes. Por ello cuando uno solicita realizar una acción y usar el recurso dentro de la aplicación salta el permiso solicitando que sea otorgado. Si es negado, la aplicación se puede explicar los beneficios de acceder a este recurso del teléfono mediante un mensaje emergente, con el mensaje se alerta al usuario que es necesario conceder el permiso para acceder al recurso y así pueda sacar partido a la aplicación.

¿QUÉ SE HACE EN EL DESARROLLO?

En el desarrollo de una aplicación móvil para Android dentro de todo el acervo que se tenga que poner en código; Está la sección de permisos en archivo manifest.xml, ahí es donde se declara los recursos de Hadware que usará. Una aplicación puede solicitar acceso, a los contactos, cámara, micrófono, calendario o GPS, entre otras.

Hay aplicaciones que pueden solicitar permisos extras; por ejemplo, nos instalamos una aplicación calculadora y esta nos pide permiso de acceso a GPS, nos hacemos la gran pregunta: ¿Para que una calculadora necesita nuestro GPS? En una nota publicada por cnnespañol (Aplicaciones de Android recolectan tus datos incluso si les dijiste que no, dice estudio) publicada el 10 julio del 2019, explaya como las aplicaciones recopilan información a pesar de que el usuario haya denegado el permiso.

Es cierto que en ocasiones como desarrolladores de aplicaciones móviles necesitamos acceder a los recursos con las que el equipo ya cuenta. Por ejemplo: un editor de fotos necesita acceder a la cámara para tomar la foto y luego llamará a las funciones de la aplicación para editarlo y finalmente solicitud de acceso a los archivos de imagen (Galería) donde almacenará la imagen. Usando la misma aplicación podemos agregar una imagen de nuestra galería, se edita y luego lo guardaremos en nuestro teléfono. Si queremos añadir más funcionalidad a esta aplicación, podemos colocar la opción de

compartir la foto editada en redes sociales, aquí debemos incluir la API de la red social que queremos postear y para ello necesitamos acceso a internet, una red wifi o datos; entonces los permisos solicitados fueron (cámara, archivos, Internet) y eso es suficiente.

Qué pasa si mi aplicación no tiene para compartir en redes sociales y sin embargo solicita acceso a mis contactos e internet, habría que especular que dicha aplicación no es segura o está accediendo a mi información por razones ajenas.

DEMOSTRACIÓN

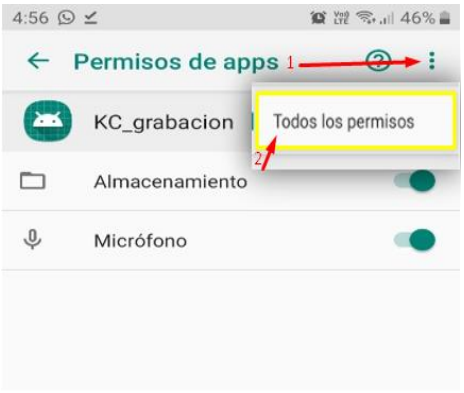


Ilustración 1, Fuente Propia

Muestro aquí una aplicación de grabación y sus permisos para que se entienda el contexto del que les hablo. Nótese en la *Ilustración 1*, los permisos para una aplicación de grabaciones de audio, la misma solicita acceso a almacenamiento, y micrófono, nada fuera de lo común.

Qué pasa si nosotros detenemos a ver en la opción todos los permisos (*Ilustración 1*).

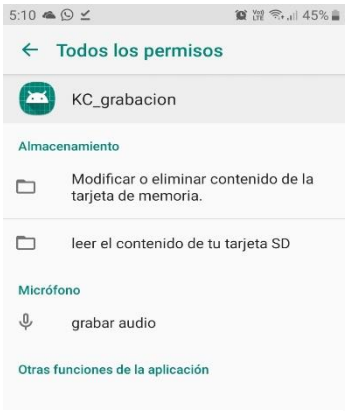


Ilustración 2, Fuente Propia

Aquí notamos lo que realmente involucra el permiso "Almacenamiento", *Ilustración 2*, el acceso a los archivos, su modificación y adicionalmente el audio.

Claro cuando una persona graba un audio, lo puede guardar, por ende, se modifica los archivos de dicha carpeta o lo puede eliminar.

RECOMENDACIÓN

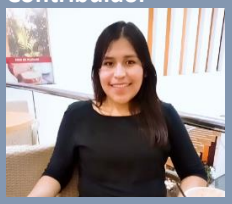
Para que una aplicación ejecute al 100% necesitamos solicitar todos los permisos que están involucrado a ella, por las razones de funcionalidad, pero ir más allá de obtener información personal creo que los usuarios no se sentirán a gusto sabiendo que su información es tomada y revisada sin su permiso.

A los usuarios, tomarse un tiempo para revisar los permisos antes de instalar una aplicación en nuestro equipo Móvil por vuestra seguridad, si hay solicitud de permisos extra, consultar con soporte o de lo contrario buscar alternativas de aplicaciones que realicen la misma tarea.

FUENTE DE REFERENCIA

- Android: https://developer.android.com/guide/topics/permissions/overview

Contribuidor



Elizabeth Quispe Esteban: Profesional informática, analista y gestor de servicios de TI, gran apasionada de la tecnología, software y Java; ITIL y TOEFL certified. Contribuyente en causas humanistas.

LinkedIn: www.linkedin.com/in/elizabeth-quispe-esteban-99543074

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen