Google publicó hoy en su blog que recomienda a los desarrolladores de aplicaciones móviles que cifren los datos que sus aplicaciones generan en los dispositivos de los usuarios, especialmente cuando utilizan almacenamiento externo sin protección que es propenso a secuestros.

Además, debido a que no existen muchos marcos de referencia disponibles para esto, Google aconsejó usar una biblioteca de seguridad fácil de implementar disponible como parte de su paquete de software Jetpack.

La biblioteca de código abierto Jetpack Security, también conocido como JetSec, permite a los desarrolladores de apps de Android, leer y escribir fácilmente archivos cifrados siguiendo las mejores prácticas de seguridad, incluido el almacenamiento de claves criptográficas y la protección de archivos que pueden contener datos confidenciales, claves API, tokens OAuth.

Android ofrece a los desarrolladores dos formas distintas de almacenar los datos de la aplicación. El primero es el almacenamiento específico de la aplicación, también conocido como almacenamiento interno, donde los archivos se almacenan en una carpeta de espacio aislado diseñada para el uso de una aplicación específica e inaccesible para otras aplicaciones en el mismo dispositivo.

El otro es el almacenamiento compartido, también conocido como almacenamiento externo, que se encuentra fuera de la protección de sandbox y por lo general se utiliza para almacenar archivos multimedia y de documentos.

Sin embargo, se ha descubierto que la mayoría de las aplicaciones usan almacenamiento externo para guardar datos confidenciales y privados de los usuarios y no toman las medidas adecuadas para protegerlas de otras aplicaciones, lo que permite a los hackers robar fotos y videos, así como manipular archivos, mediante una técnica denominada *Media File Jacking.*

Las consecuencias de esto se demostraron hace dos años con los ataques man-in-the-desk, que hacen posible que los atacantes comprometan una aplicación al manipular algunos datos que se intercambian entre ella y el almacenamiento externo.

Otra investigación demostró un ataque de canal lateral mediante el que los hackers pueden tomar fotos y grabar videos en secreto, aún cuando no tienen permisos específicos del dispositivo para hacerlo, sino solo para aprovechar el acceso al almacenamiento externo del dispositivo.

Para evitar estos ataques, Android 10 cuenta con una característica llamada Scoped Storage, que también almacena los datos de cada aplicación en el almacenamiento externo, lo que limita el acceso de las aplicaciones a los datos guardados por otras apps en el dispositivo. Pero la biblioteca JetSec va más adelante con una solución fácil de usar para cifrar datos para un nivel adicional de protección.

> *«Si su aplicación utiliza almacenamiento compartido, debe cifrar los datos. En el directorio de inicio de la aplicación, su aplicación debe encriptar datos si la aplicación maneja información confidencial que incluye, entre otros, información de identificación personal (PII), registros de salud, detalles financieros o datos empresariales»*, dice Google.

La compañía también recomendó que los desarrolladores de aplicaciones combinen el cifrado con información biométrica para mayor seguridad y privacidad.

La biblioteca de Jetpack Security tuvo su vista previa en mayo pasado, en su conferencia anual de desarrolladores. Viene como parte de una expansión de Android Jetpack, una colección de componentes de software de Android que ayuda a los desarrolladores a seguir las mejores prácticas y diseñar aplicaciones de alta calidad.