UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA:

Mecanismos de cifrado de datos en aplicaciones móviles

PRESENTADO POR:

Pliego Cortes Giovanni

GRUPO:

10 ° B

MATERIA:

Desarrollo móvil integral

CARRERA:

TI. Desarrollo de software multiplataforma

Docente:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 23 de enero del 2025

El cifrado de datos en aplicaciones móviles es un componente esencial para garantizar la seguridad de la información sensible de los usuarios. Esta práctica protege los datos frente a accesos no autorizados, tanto cuando están almacenados en el dispositivo como durante su transmisión a través de redes. Dependiendo del caso, se pueden emplear diversos mecanismos y estrategias que varían según el nivel de seguridad requerido y la arquitectura de la aplicación.

El cifrado en reposo protege los datos almacenados localmente en el dispositivo, como bases de datos, archivos o configuraciones críticas. Para ello, los sistemas operativos móviles ofrecen herramientas nativas. En iOS, la API de Protección de Datos y el Keychain son las principales opciones para implementar cifrado de archivos y almacenar claves de manera segura. Por su parte, en Android, el sistema Keystore permite manejar claves criptográficas y emplear algoritmos como AES o RSA. Además, existen bibliotecas como SQLCipher, que cifran bases de datos SQLite de forma eficaz, asegurando que incluso si un atacante obtiene acceso físico al almacenamiento, los datos estarán protegidos por una capa de cifrado.

Por otro lado, el cifrado en tránsito resguarda la información mientras se transmite entre la aplicación y los servidores. El uso de TLS (Transport Layer Security) garantiza comunicaciones seguras mediante HTTPS, previniendo ataques de intermediarios como el "man-in-the-middle" (MITM). Para reforzar esta seguridad, se puede implementar la técnica de *certificate pinning*, que verifica que los certificados utilizados en las conexiones coincidan con un conjunto previamente definido, reduciendo la posibilidad de que se acepten certificados no confiables.

Las claves y credenciales también representan un punto crítico de vulnerabilidad en las aplicaciones móviles. Estas deben almacenarse y manejarse con especial cuidado. En iOS, el Keychain actúa como un almacén cifrado para credenciales, mientras que en Android, el Keystore cumple una función similar. Además, la tokenización sustituye datos sensibles como números de tarjetas por identificadores irreversibles, dificultando su explotación en caso de ser interceptados. Para proteger contraseñas, se utiliza la técnica de *hashing* con

algoritmos como SHA-256 o bcrypt, a menudo complementados con *salts* únicas para prevenir ataques de fuerza bruta o de diccionario.

El cifrado a nivel de aplicación es otra estrategia común, donde los desarrolladores integran algoritmos criptográficos directamente en la lógica de la aplicación. Los algoritmos simétricos como AES son ideales para cifrar y descifrar datos con una clave compartida, mientras que los algoritmos asimétricos como RSA o ECC son útiles para escenarios donde se requiere una clave pública para cifrar y una clave privada para descifrar. Una práctica moderna es combinar ambos enfoques en lo que se conoce como cifrado híbrido, que utiliza la eficiencia de AES y la seguridad de RSA.

Además de estos mecanismos, hay una serie de recomendaciones generales para maximizar la seguridad. Es fundamental evitar almacenar claves directamente en el código fuente de la aplicación. En su lugar, las claves pueden derivarse de valores dinámicos o almacenarse en los sistemas seguros del dispositivo. La rotación periódica de claves y la implementación de ofuscación del código fuente también son esenciales para mitigar riesgos. Por último, realizar auditorías de seguridad y pruebas de penetración regularmente asegura que la aplicación cumpla con los estándares más altos de protección.

En resumen, el cifrado de datos es una práctica integral en el desarrollo de aplicaciones móviles. Con la combinación adecuada de herramientas, algoritmos y buenas prácticas, es posible proteger tanto la información de los usuarios como la integridad de las aplicaciones frente a amenazas.