Universidad Tecnológica de Tijuana

TEMA:

Mecanismo de cifrado de datos en aplicaciones moviles

PRESENTADO POR:

Sánchez Zamudio Guadalupe

GRUPO:

10B BIS

MATERIA:

Desarrollo movil integral

PROFESOR:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 24 de enero del 2025

El cifrado de datos en aplicaciones móviles es esencial para proteger la información sensible de los usuarios frente a accesos no autorizados y posibles vulnerabilidades. Este proceso convierte los datos en un formato ilegible para cualquier persona o aplicación que no posea la clave de descifrado adecuada.

Cifrado en dispositivos Android e iOS

Tanto Android como iOS implementan mecanismos de cifrado para salvaguardar la información almacenada en los dispositivos:

- **Android:** Ofrece la opción de cifrar tanto el dispositivo como la tarjeta SD. Al activar el cifrado, se requiere que el usuario establezca una contraseña alfanumérica para desbloquear la pantalla. Es recomendable mantener el dispositivo conectado a la corriente durante el proceso de cifrado, ya que puede durar aproximadamente una hora y no debe interrumpirse.
- **iOS:** Utiliza una clave única de 256 bits, conocida como UID, almacenada en el hardware del dispositivo. Esta clave se combina con el código de acceso del usuario para generar una clave de acceso que protege los datos. A diferencia de Android, la UID no puede ser extraída del dispositivo, lo que previene intentos de fuerza bruta para obtener la contraseña. Además, iOS cifra cada archivo con una clave específica, que a su vez está protegida por la clave del sistema de archivos y el UID de hardware.

Prácticas recomendadas para el cifrado en aplicaciones móviles

Para garantizar una protección efectiva de los datos en aplicaciones móviles, se sugieren las siguientes prácticas:

- Almacenamiento seguro: Evitar guardar información sensible en el almacenamiento local del dispositivo. Si es necesario, cifrarla utilizando una clave derivada del hardware de almacenamiento seguro, que requiera autenticación previa.

Gestión de claves criptográficas:

- No depender únicamente de criptografía simétrica cuyas claves se encuentren directamente en el código fuente de la aplicación.
- No reutilizar una misma clave criptográfica para varios propósitos.
- Generar valores aleatorios utilizando un generador de números aleatorios suficientemente seguro.

Autenticación y control de sesiones:

- Implementar mecanismos de autenticación robustos, como la autenticación biométrica o de doble factor, especialmente en aplicaciones que manejan información muy sensible.
- Establecer tiempos de expiración para sesiones y tokens tras un período de inactividad del usuario.
- Comunicación segura: Asegurar que la información se envíe cifrada utilizando el protocolo TLS. La aplicación debe verificar el certificado del sistema remoto al establecer el canal seguro y aceptar solo certificados firmados por una autoridad de certificación de confianza.

Importancia del cifrado en aplicaciones móviles

El cifrado de datos es fundamental para proteger la información confidencial almacenada en una aplicación móvil. Al utilizar técnicas de cifrado, se garantiza que los datos sean ilegibles para personas o aplicaciones no autorizadas, lo que previene accesos no deseados y posibles vulnerabilidades.

Bibliografías:

- Seidor. (s.f.). *Importancia de la seguridad en aplicaciones móviles y cómo garantizarla*. Recuperado de https://www.seidor.com/es-es/blog/importancia-seguridad-aplicaciones-moviles-como-garantizarla

- Universidad Veracruzana. (s.f.). *Cifrado en dispositivos móviles Android e iOS*. Recuperado de https://www.uv.mx/infosegura/general/noti_cifrado/

- Seidor. (s.f.). *Seguridad en aplicaciones móviles: Cómo proteger tus datos y dispositivos*. Recuperado de https://www.seidor.com/es-es/blog/seguridad-aplicaciones-moviles