UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

Assignment:

Mecanismos de cifrado de datos en aplicaciones móviles

BY:

Daniel Chavez Madrigal

GROUP:

9-B

SUBJECT:

Desarrollo Móvil Integral

PROFESSOR:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 24 de enero del 2025

El cifrado de datos en aplicaciones móviles es una práctica esencial para proteger la información sensible de los usuarios y garantizar la seguridad de las comunicaciones. Este proceso implica convertir datos legibles en un formato codificado que solo puede ser descifrado por aquellos que poseen la clave adecuada. En el contexto de las aplicaciones móviles, el cifrado se utiliza tanto para proteger los datos en tránsito como los datos en reposo.

Cifrado de Datos en Tránsito y en Reposo: El cifrado de datos en tránsito se refiere a la protección de la información mientras se transmite entre el dispositivo del usuario y los servidores. Esto se logra mediante el uso de protocolos como TLS (Transport Layer Security), que aseguran que los datos no puedan ser interceptados y leídos por terceros durante su transmisión. Por otro lado, el cifrado de datos en reposo implica proteger la información almacenada en el dispositivo móvil, utilizando algoritmos robustos como AES (Advanced Encryption Standard) para garantizar que los datos permanezcan seguros incluso si el dispositivo es comprometido.

Autenticación Segura: La autenticación es un componente crucial de la seguridad en aplicaciones móviles. La implementación de métodos de autenticación multifactor (MFA) y biométrica (como huellas dactilares y reconocimiento facial) añade capas adicionales de seguridad, dificultando el acceso no autorizado. Estos métodos aseguran que solo los usuarios legítimos puedan acceder a la aplicación y sus datos.

Normas y Mejores Prácticas: Organizaciones como OWASP (Open Web Application Security Project) han desarrollado guías y listas de verificación, como el OWASP Mobile Top 10, que destacan las principales vulnerabilidades de seguridad en aplicaciones móviles y ofrecen recomendaciones para mitigarlas. Además, la norma ISO/IEC 27001 proporciona un marco para la gestión de la seguridad de la información, incluyendo aspectos específicos para aplicaciones móviles.

Seguridad de API: Las API (Interfaces de Programación de Aplicaciones) son esenciales para la funcionalidad de muchas aplicaciones móviles, pero también representan un punto de vulnerabilidad. Es crucial implementar medidas de seguridad como autenticación, autorización y límites de velocidad para proteger las API contra el acceso no autorizado y los ataques.

Transmisión Segura de Datos: La implementación de TLS no solo asegura la transmisión de datos entre el servidor y la aplicación, sino que también implica la

verificación constante del certificado SSL del servidor para prevenir ataques de intermediarios. Esto garantiza que los datos no sean interceptados o alterados durante su transmisión.

Validación de Entrada de Usuario: La validación y desinfección de las entradas de usuario son prácticas esenciales para prevenir ataques comunes como inyecciones de SQL y scripting entre sitios (XSS). Estas técnicas aseguran que los datos ingresados por los usuarios no puedan ser utilizados para comprometer la seguridad de la aplicación.

Gestión de Claves de Cifrado: Las claves de cifrado son fundamentales para la seguridad de los datos cifrados. Es vital gestionar y proteger estas claves adecuadamente para evitar vulnerabilidades en el sistema de cifrado. Esto incluye el uso de almacenes de claves seguros y la rotación regular de las claves.

Referencias:

Nativapps. (2024, December 18). *Mejores prácticas de seguridad para aplicaciones móviles*. NativApps Inc. https://nativapps.com/mejores-practicas-de-seguridad-para-aplicaciones-moviles/

Vargas, J., & Vargas, J. (2025, January 4). *Cómo implementar el cifrado en aplicaciones móviles*. cyberestetica.com. https://cyberestetica.com/como-implementar-el-cifrado-en-aplicaciones-moviles/