Materia:

Desarrollo móvil Integral

Grupo:

10-B

Nombre del Alumno:

Rendon Gurrola Alan Misael

Docente:

Antonio Reyes Perez

Fecha de Elaboración:

24/01/2024

Mecanismos de cifrado de datos en aplicaciones móviles

¿Qué es el Cifrado de Datos?

El cifrado de datos es el proceso de transformar la información digital de texto sin formato en un formato incomprensible conocido como texto cifrado. Este proceso de codificación (transformación) de datos utiliza lo que se conoce como “key” – una pieza de información, generalmente números y/o letras, generada por un algoritmo criptográfico (un conjunto de reglas).

La información cifrada solo puede ser leída (descifrada de nuevo en formato legible) por alguien con una clave de descifrado.

Aunque el cifrado no impide por sí solo que los ataques cibernéticos accedan a un sistema, hace que los datos que se guardan en el sistema o los datos que se transmiten sean seguros para cualquier persona que pueda accederlos o interceptarlos.

Métodos de Cifrado

En general, hay dos métodos de cifrado:

Cifrado simétrico utiliza una sola clave para cifrar y descifrar datos

Cifrado asimétrico o de clave pública utiliza una clave separada para cifrar y descifrar datos. La clave de cifrado se conoce como clave pública; la clave de descifrado se conoce como clave privada.

Estándares Comunes de Cifrado

La fuerza del cifrado depende del algoritmo que se utilice, el tamaño de la clave, la generación de la clave y el proceso de intercambio de claves.

1. Data Encryption Standard (DES) – Ahora en desuso

Un algoritmo de clave simétrica de 56 bits de longitud. Desarrollado a principios de la década de 1970, esto se considera un estándar débil debido a su tamaño de clave corto.

2. Triple DES – Ahora en desuso

También conocido como TDES, 3DES o Triple DEA, este es un cifrado de bloque de clave simétrica que aplica el algoritmo de cifrado DES tres veces a cada bloque de datos, pero aún con una longitud de clave de 56 bits. El Instituto Nacional de Estándares y Tecnología (NIST) ha desaprobado DES y 3DES para nuevas aplicaciones y requiere una eliminación gradual de todas las aplicaciones para 2023.

3. RSA

Un sistema de cifrado de clave pública llamado así por sus fundadores, con la clave pública basada en dos números primos grandes (secretos) junto con un valor auxiliar, con los primos secretos necesarios para el descifrado. Se usa comúnmente para aplicaciones que requieren firmas digitales.

4. Estándares Avanzados de Cifrado (AES)

También conocido como Rijndael, un algoritmo de clave simétrica y variante del cifrado de bloques del mismo nombre, AES es el estándar adoptado por el Gobierno de los Estados Unidos /NIST. AES aprovecha una familia de cifrados con diferentes tamaños de clave y bloque. La mayoría de las herramientas de cifrado se basan en el cifrado AES.

5. Blowfish y Twofish

Aunque solo tiene un tamaño de bloque de 64 bits, Blowfish es popular en el desarrollo de software, específicamente para bases de datos y cifrado de archivos. Twofish es un algoritmo de cifrado simétrico creado para reemplazar Blowfish, que utiliza un tamaño de bloque de 128 bits y admite claves más grandes que son más resistentes a los ataques de fuerza bruta.

Saber qué tipo de cifrado usar se trata de elegir una opción segura – y eso cambiará con el tiempo a medida que los algoritmos evolucionen al panorama de riesgo emergente –, pero también la opción correcta para la aplicación. Por ejemplo, cuanto mayor sea la clave, más segura será –, pero también mayor será la posibilidad de que el rendimiento se vea afectado.

¿Por qué Proteger los Datos de Aplicaciones Móviles y Web?

Web y empresas de desarrollo de aplicaciones móviles debe priorizar la privacidad de los datos y el cumplimiento de acuerdo con varias regulaciones estrictas – o enfrentar no solo una erosión de la confianza con sus usuarios y daños de marca potencialmente irreversibles, sino también multas significativas.

Además, en el caso de la seguridad de las aplicaciones móviles, el hecho de que el código se ejecute desde el sistema operativo del punto final (dispositivo móvil) introduce riesgos para la propiedad intelectual (IP).

¿Por Qué la Seguridad de la Aplicación Web es Diferente de la Seguridad de la Aplicación Móvil?

Aunque tanto una aplicación web como una aplicación móvil se accede desde un dispositivo móvil o teléfono inteligente, la arquitectura de cada aplicación es significativamente diferente –, lo que afecta el enfoque del cifrado de datos y las otras herramientas y prácticas disponibles para mejorar la seguridad de la aplicación móvil.

Una aplicación web es un sitio web dinámico, que cambia la pantalla en función de las entradas o acciones del usuario final, pero la aplicación se ejecuta en un servidor con solo una pequeña parte de la aplicación accesible para el usuario final (el front-end).

Debido a esto, las herramientas de seguridad tradicionales, como los firewalls, pueden agregar capas de protección a los datos en una aplicación web.

Las aplicaciones web aprovechan las capas de socket seguro (SSL) y la seguridad de la capa de transporte (TLS) para establecer enlaces cifrados entre computadoras en red. El certificado SSL (certificado TLS) es un certificado digital (certificado de clave pública) que autentica la identidad de un sitio web y establece esa conexión de cifrado entre un servidor web y un navegador.

Una aplicación móvil, por el contrario, se descarga e instala en un dispositivo móvil – un proceso que aumenta la superficie de ataque de una instancia (el servidor) a muchos endpoints (cada dispositivo móvil) – endpoints sobre los cuales el desarrollador no tiene control de seguridad.

Este aumento de la superficie de ataque se combina con la mayor cantidad de datos recopilados y almacenados por el dispositivo móvil (vs el navegador).

Una aplicación móvil es más vulnerable a que se descubran vulnerabilidades y se introduzcan compromisos o se infiltre en la comunicación entre la aplicación y los sistemas de back-end para obtener acceso a un conjunto más amplio de datos confidenciales.

BIBLIOGRAFIA

Sharma, R. K. (2024, febrero 16). *How to use data encryption to protect your mobile apps & websites*. Net Solutions. https://www.netsolutions.com/hub/mobile-app-development/data-encryption