Apuntes TLS

Contenido

Definición de TLS

TLS (Transport Layer Security) es un protocolo criptográfico que se utiliza para garantizar la seguridad y privacidad de la comunicación en línea. El objetivo principal de TLS es proteger la integridad de los datos, asegurando que la información no se pueda interceptar, modificar o falsificar durante la transmisión.

TLS es la versión más reciente del protocolo SSL (Secure Sockets Layer). La versión más comúnmente utilizada es TLS 1.2, aunque TLS 1.3 es la versión más reciente y segura.

¿Que Sistema Utiliza TLS para el cifrado de datos?

TLS utiliza un sistema de clave pública y privada para cifrar la comunicación entre dos dispositivos. La clave pública se utiliza para cifrar los datos, mientras que la clave privada se utiliza para descifrarlos.

TLS también utiliza certificados digitales para autenticar los servidores y garantizar que el destinatario sea el correcto. Estos certificados son emitidos por autoridades de certificación (CA) de confianza.

En que se divide la comunicación TLS

La comunicación TLS se divide en dos fases: el establecimiento de la conexión segura y la transferencia de datos segura. Durante la fase de establecimiento de la conexión segura, se establece una sesión segura entre el cliente y el servidor. Durante la fase de transferencia de datos segura, se cifran los datos que se transmiten entre el cliente y el servidor:

Ejemplos de Protocolos

TLS es compatible con una variedad de protocolos de aplicación, incluyendo HTTPS (HTTP seguro), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3) y IMAP (Internet Message Access Protocol).

TLS ha sido diseñado para resistir a una variedad de ataques, como la suplantación de identidad, la interceptación de datos y la inyección de datos maliciosos.

En resumen, TLS es un protocolo criptográfico fundamental para garantizar la seguridad y privacidad de la comunicación en línea. Utiliza un sistema de clave pública y privada, certificados digitales y una variedad de medidas de seguridad para proteger la integridad de los datos durante la transmisión.

Cypher suits

Deficinicion Cipher suits

Los cipher suites (conjuntos de cifrado) son una combinación de algoritmos de cifrado, de intercambio de claves y de autenticación que se utilizan para proteger la comunicación en línea mediante el protocolo TLS

Los cipher suit con distintos tipos de cifrado:

Con clave simétrica:

Cipher suites con algoritmo de cifrado simétrico: estos cipher suites utilizan un algoritmo de cifrado simétrico, como AES o 3DES, para cifrar los datos. La clave de cifrado se intercambia utilizando un algoritmo de intercambio de claves asimétrico, como RSA o Diffie-Hellman.

Con clave asimétrica:

Cipher suites con algoritmo de cifrado asimétrico: estos cipher suites utilizan un algoritmo de cifrado asimétrico, como RSA o ECC, para cifrar los datos. El proceso de intercambio de claves también se realiza utilizando el mismo algoritmo de cifrado asimétrico.

¿Que utilizan los cipher suit para certificarse?

Cipher suites con autenticación basada en certificados: estos cipher suites utilizan certificados digitales para autenticar los servidores y garantizar que el destinatario sea el correcto. El certificado digital contiene la clave pública del servidor y es emitido por una autoridad de certificación de confianza

Cipher suites con autenticación basada en contraseñas: estos cipher suites utilizan contraseñas o claves compartidas para autenticar a los clientes y servidores. Este tipo de cipher suite es menos seguro que aquellos que utilizan autenticación basada en certificados.

Cipher suites con autenticación basada en tokens: estos cipher suites utilizan tokens o tarjetas inteligentes para autenticar a los clientes y servidores. Este tipo de autenticación es más segura que la autenticación basada en contraseñas, ya que los tokens son difíciles de duplicar o falsificar.

Es importante tener en cuenta que la elección del cipher suite adecuado dependerá del nivel de seguridad requerido por la aplicación en particular. Los cipher suites más seguros suelen ser aquellos que utilizan algoritmos de cifrado simétrico y asimétrico, autenticación basada en certificados y protocolos de intercambio de claves como Diffie-Hellman.

Diffie Hellman

Definición

El protocolo de intercambio Diffie-Hellman es un algoritmo de cifrado de clave pública que permite a dos partes, que no se conocen previamente, intercambiar una clave secreta a través de un canal de comunicación inseguro. Este protocolo fue desarrollado por Whitfield Diffie y Martin Hellman en 1976 y se considera una de las técnicas fundamentales de la criptografía moderna.

¿En que se basa el protocolo Diffie_Hellman?

El protocolo de intercambio Diffie-Hellman se basa en la idea de que dos partes pueden generar una clave secreta compartida sin transmitirla a través del canal de comunicación inseguro. Para lograr esto, se utilizan dos números primos grandes y un número secreto elegido por cada parte. Estos números se utilizan para generar una clave secreta compartida que se utiliza para cifrar y descifrar los datos.

Explicación del Protocolo

Cada parte elige un número secreto aleatorio (a y b, respectivamente) y dos números primos grandes (p y g). Estos números se comparten públicamente.

Cada parte calcula su clave pública, que es g elevado a su número secreto, módulo p. Es decir, A = g^a mod p y B = g^b mod p.

Cada parte intercambia su clave pública con la otra parte

Cada parte calcula la clave secreta compartida utilizando la clave pública de la otra parte y su propio número secreto. Es decir, A calcula K = B^a mod p y B calcula K = A^b mod p.

La clave secreta compartida K puede utilizarse para cifrar y descifrar los datos que se transmiten entre las dos partes.

Una de las ventajas del protocolo de intercambio Diffie-Hellman es que, incluso si un atacante intercepta la comunicación entre las dos partes, no puede determinar la clave secreta compartida sin conocer los números secretos de ambas partes. Esto hace que sea muy difícil para los atacantes descifrar la comunicación.

Sin embargo, es importante tener en cuenta que el protocolo de intercambio Diffie-Hellman por sí solo no proporciona autenticación. Es decir, no garantiza que la otra parte sea realmente quien dice ser. Por lo tanto, se recomienda utilizar el protocolo de intercambio Diffie-Hellman

junto con autenticación basada en certificados para garantizar la seguridad y privacidad de la comunicación.