TLS1.3: ¿Qué hay de nuevo? (Parte II)

Por mikiminoru el 19 nov 2020 con 0 comentarios

En este segundo post vamos a describir cómo se inician las conexiones a través de TLS1.3.

El handshake tiene una estructura diferente, y más rápida en comparación con las versiones anteriores. En este caso las etapas que se producen son:

1. El cliente genera la clave para el intercambio

2. El cliente envía el ClientHello, en el que se encuentra la siguiente información:
2.1. Una lista de las suites de cifrado que acepta
2.2. Una lista de claves públicas para realizar el intercambio de claves.
2.3. Versiones del protocolo que acepta el cliente.

3. El servidor genera las claves para el intercambio.

4. El servidor envía el ServerHello de vuelta, con los siguientes datos:
4.1. La suite de cifrado elegida
4.2. La clave pública elegida para el intercambio de claves
4.3. La versión del protocolo

5. Claves del handshake del servidor. Para cifrar el resto del handshake usa:
5.1. Clave pública del cliente
5.2. Clave privada del servidor
5.3. SHA256 del ClientHello y del ServerHello

El servidor calcula la clave secreta compartida, que es calculada a partir de ambos intercambio de claves (a través del algoritmo de curva elíptica curve25519 de Diffie Hellman).

6. Claves del handshake del cliente. El cliente usa:
6.1. La clave pública del servidor.
6.2. La clave privada del cliente.
6.3. El hash del SHA256 del ClientHello y del ServerHello

El cliente calcula la clave secreta compartida (de la misma forma que el servidor en el paso anterior)

7. El servidor envía el certificado.

8. El servidor envía una verificación del certificado en la que se enlaza la clave usada en el intercambio de claves, para confirmar su integridad.

9. El servidor termina comprobando que el proceso no se ha visto alterado, de forma que realiza un hash SHA256 resultante de todos los mensajes que forman el handshake (desde el paso 2 hasta el paso 8).

10. El servidor calcula las claves que serán usadas para cifrar el tráfico durante la sesión. Para ello usa:
10.1. La clave secreta del handshake
10.2. El hash resultante del paso 9

En este paso se realizan una serie de operaciones de las que resultan las claves de la aplicación para el cliente y el servidor.

11. El cliente realiza las mismas operaciones que el servidor en el paso anterior (obteniendo, por supuesto, los mismos valores para las claves).

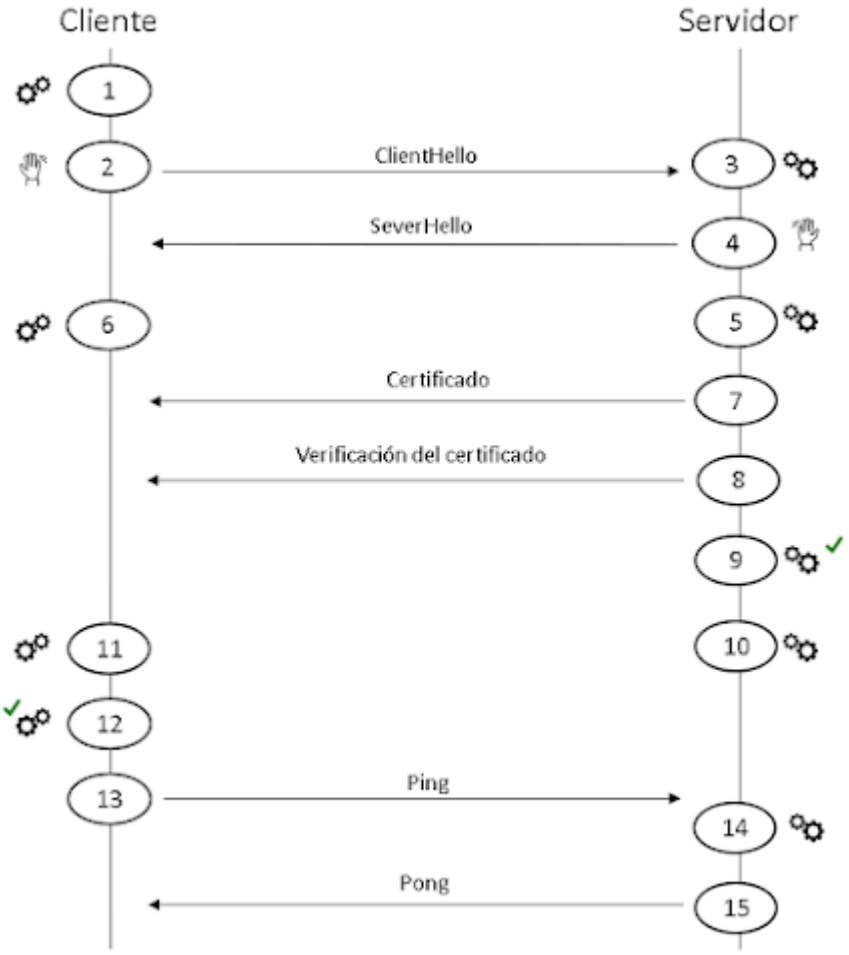
12. El cliente da por terminado el handshake, y realiza el hash SHA256 resultante de todos los mensajes que forman el handshake (desde el paso 2 hasta el paso 8).

13. El cliente manda el mensaje “ping” al servidor

14. El servidor crea las claves de sesión para cifrar la conexión.

15. El servidor manda el mensaje “pong” al cliente.

De forma esquematizada, podemos visualizar este proceso en el siguiente esquema:



Para un mayor nivel de detalle del handshake, podéis consultar el siguiente enlace: https://tls13.ulfheim.net/

Esperamos que hayáis descubierto algunas de las curiosidades con las que ha venido esta nueva versión de TLS.

Muchos maullidos!

M

OPENSSL , SSL , TLS

Otros artículos relacionados

TLS1.3: ¿Qué hay de nuevo? (Parte I)

30 DE OCTUBRE DE 2020

Suites de TLS/SSL (Parte III)

21 DE SEPTIEMBRE DE 2020

Suites de TLS/SSL (Parte IV)

22 DE SEPTIEMBRE DE 2020

Suites de cifrado TLS/SSL (Parte II)

15 DE SEPTIEMBRE DE 2020