Introducción SSL con la transacción y el intercambio de paquetes de la muestra

Contenido

Introducción

Este documento describe los conceptos básicos de protocolo de Secure Sockets Layer (SSL) y proporciona una transacción y a una captura de paquetes de la muestra.

Descripción del expediente SSL

La unidad básica de datos en el SSL es un expediente. Cada expediente consiste en una encabezado de registro del octeto cinco, seguida por los datos.

Formato de registro

- Tipo: uint8 - valores enumerados abajo
- Versión: uint16
- Longitud: uint16

Tipo	Versión		Longitud	
T	VH	VL	LH	LL

Tipo de registro

Hay cuatro tipos de registro en el SSL:

- **Apretón de manos** (22, 0x16)
- **Cambie espec. de la cifra** (20, 0x14)
- **Alerte** (21, 0x15)
- **Datos de aplicación** (23, 0x17)

Registre la versión

La versión de registro es un valor 16-byte y se formata en la orden de red.

> Nota: Para el SSL versión 3 (SSLv3), la versión es 0x0300. Para la versión 1 (TLSv1) de Transport Layer Security, la versión es 0x0301. El dispositivo de seguridad adaptante de Cisco (ASA) no soporta la versión del SSL versión 2 (SSLv2), que utiliza la versión 0x0002, o cualquier de TLS mayor que TLSv1.

Longitud de registro

La longitud de registro es un valor 16-byte y se formata en la orden de red.

En la teoría, esto significa que un único registro puede ser hasta 65,535 (2^16 -1) bytes de largo. RFC2246 los estados TLSv1 que el Largo máximo es 16,383 (2^14 -1) bytes. Los productos Microsoft (Microsoft Internet Explorer y Servicios de Internet Information Server) se saben para exceder estos límites.

Tipos de expedientes

Esta sección describe los cuatro tipos de expedientes SSL.

Expedientes del apretón de manos

Los expedientes del apretón de manos contienen un conjunto de los mensajes que son para apretón de manos usado. Éstos son los mensajes y sus valores:

- **Hola petición** (0, 0x00)
- **Saludos del cliente** (1, 0x01)
- **Saludos del servidor** (2, 0x02)
- **Certificado** (11, 0x0B)
- **Intercambio de la clave del servidor** (12, 0x0C)
- **Pedido de certificado** (13, 0x0D)
- **Saludos del servidor hechos** (14, 0x0E)
- **El certificado verifica** (15, 0x0F)
- **Intercambio de claves del cliente** (16, 0x10)

- **Acabado** (20, 0x14)

En el caso simple, los expedientes del apretón de manos no se cifran. Sin embargo, un expediente del apretón de manos que contiene un mensaje acabado se cifra siempre, pues ocurre siempre después de que un expediente espec. de la cifra del cambio (CCS).

Cambie los expedientes espec. de la cifra

Los expedientes CCS se utilizan para indicar un cambio en las cifras crpytographic. Inmediatamente después que el expediente CCS, todos los datos se cifra con la nueva cifra. Los expedientes CCS pudieron o no pudieron ser cifrados; en una conexión simple con un solo apretón de manos, el expediente CCS no se cifra.

Expedientes de la alerta

Los expedientes de la alerta se utilizan para indicar al par que ha ocurrido una condición. Algunas alertas son advertencias, mientras que otras son fatales y hacen la conexión fallar. Las alertas pudieron o no se pudieron cifrar, y pudieron ocurrir durante un apretón de manos o durante la Transferencia de datos. Hay dos tipos de alertas:

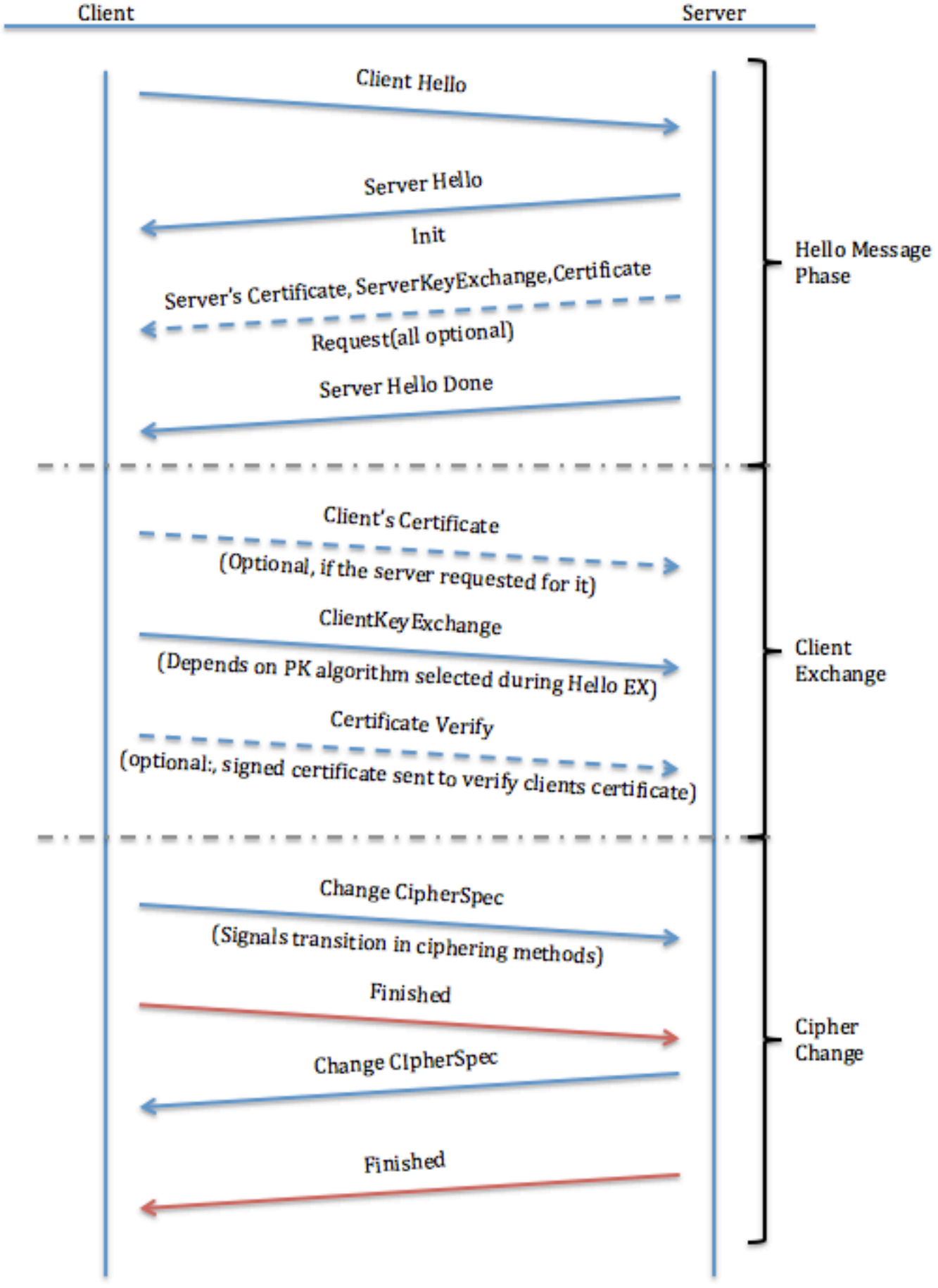
- **Alertas del cierre:** La conexión entre el cliente y el servidor se debe cerrar correctamente para evitar cualquier clase de ataques del truncamiento. Se envía un mensaje del **close_notify** que indica al beneficiario que el remitente no enviará más los mensajes en esa conexión.
- **Alertas del error:** Cuando se detecta un error, el partido de detección envía un mensaje al otro partido. Sobre la transmisión o el recibo de un mensaje de alerta fatal, ambas partes cierran inmediatamente la conexión. Algunos ejemplos de las alertas del error son:
  - **unexpected_message** (fatal)
  - **decompression_failure**
  - **handshake_failure**

Expediente de datos de aplicación

Estos expedientes contienen los datos de aplicación real. Estos mensajes son llevados por la capa de registro y hechos fragmentos, comprimidos, y cifrados, sobre la base del estado de la conexión actual.

Transacción de la muestra

Esta sección describe una transacción de la muestra entre el cliente y servidor.



El intercambio hello

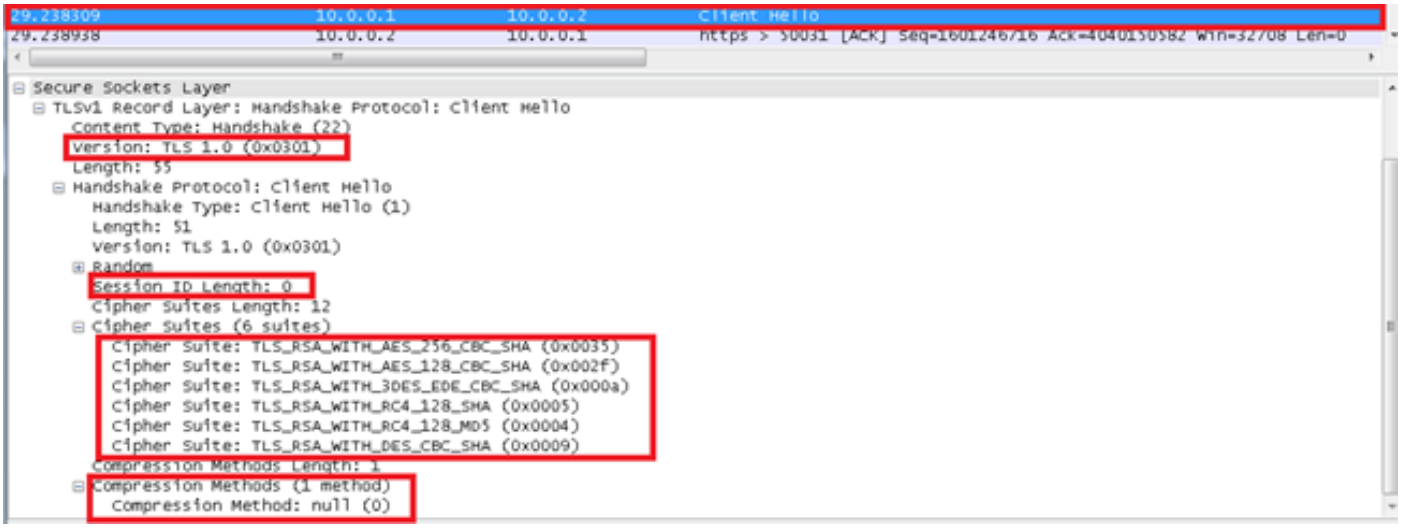
Cuando un cliente SSL y un servidor comienzan al communitcate, están de acuerdo con una Versión del protocolo, los algoritmos criptográficos selectos, se autentican opcionalmente, y utilizan las técnicas de la encripción de clave pública para generar los secretos compartidos. Estos procesos se realizan en el protocolo de entrada en contacto. En resumen, el cliente envía un mensaje de los saludos del cliente al servidor, que debe responder con un mensaje de los saludos del servidor u ocurre un error fatal y la conexión falla. Los saludos del cliente y los saludos del servidor se utilizan para establecer las capacidades de la mejora de la seguridad entre el cliente y servidor.

Saludos del cliente

El saludo del cliente envía estos atributos al servidor:

- **Versión del protocolo:** La versión del Protocolo SSL por el cual el cliente desea comunicar durante esta sesión.
- **ID de sesión:** El ID de una sesión los deseos del cliente a utilizar para esta conexión. En los primeros saludos del cliente del intercambio, el ID de sesión está vacío (refiera a la captura de pantalla de la captura de paquetes después de la nota abajo).
- **Habitación de la cifra:** Esto se pasa del cliente al servidor en el mensaje de los saludos del cliente. Contiene las combinaciones de algoritmos criptográficos soportados por el cliente en orden de la preferencia del cliente (primera opción primero). Cada habitación de la cifra define un Key Exchange Algorithm y espec. de la cifra. El servidor selecciona una habitación de la cifra o, si no se presenta ningunas opciones aceptables, vuelve una alerta del error del apretón de manos y cierra la conexión.
- **Método de compresión:** Incluye una lista de algoritmos de compresión soportados por el cliente. Si el servidor no soporta ningún método enviado por el cliente, la conexión falla. El método de compresión puede también ser nulo.

  Nota: El dirección IP del servidor en las capturas es 10.0.0.2 y el dirección IP del cliente es 10.0.0.1.



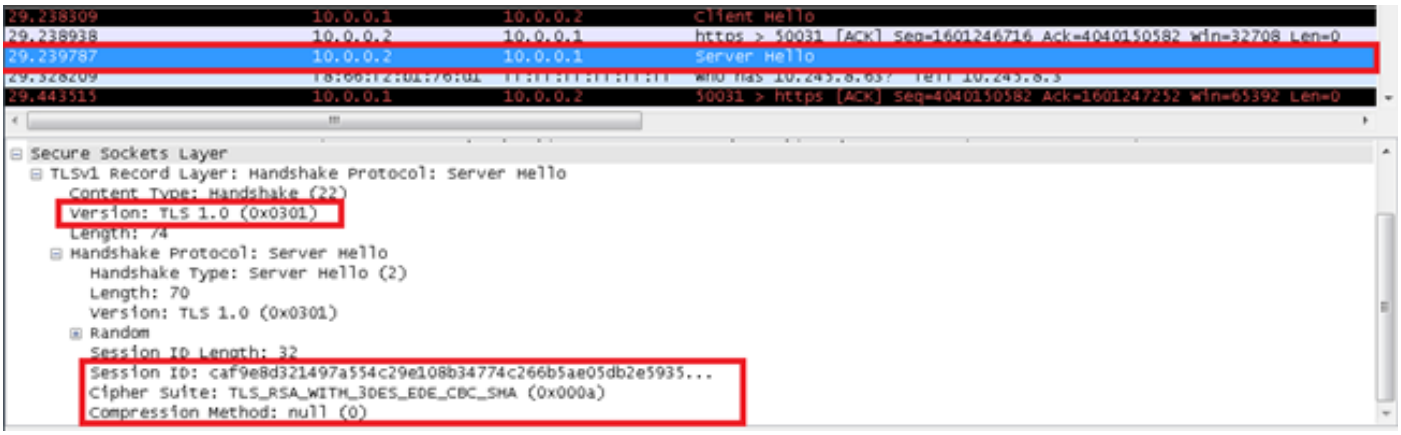
Saludos del servidor

El servidor devuelve estos atributos al cliente:

- **Versión del protocolo:** La versión elegida del Protocolo SSL que los soportes de cliente.
- **ID de sesión:** Ésta es la identidad de la sesión que corresponde a esta conexión. Si el ID de

sesión enviado por el cliente en los saludos del cliente no está vacío, el servidor mira en el caché de la sesión para una coincidencia. Si se encuentra una coincidencia y el servidor está dispuesto a establecer la nueva conexión usando el estado de la sesión especificado, el servidor responde con el mismo valor que fue suministrado por el cliente. Esto indica una sesión reanudada y dicta que los partidos deben proceder directamente a los mensajes acabados. Si no, este campo contiene un diverso valor que identifique la nueva sesión. El servidor pudo volver un **session_id** vacío para indicar que la sesión no será ocultada, y por lo tanto no puede ser reanudado.

- **Habitación de la cifra:** Según lo seleccionado por el servidor de la lista que fue enviada del cliente.
- **Método de compresión:** Según lo seleccionado por el servidor de la lista que fue enviada del cliente.
- **Pedido de certificado:** El servidor envía el cliente una lista de todos los Certificados que se configuran en ella, y permite que el cliente seleccione que la certifican quiere utilizar para la autenticación.

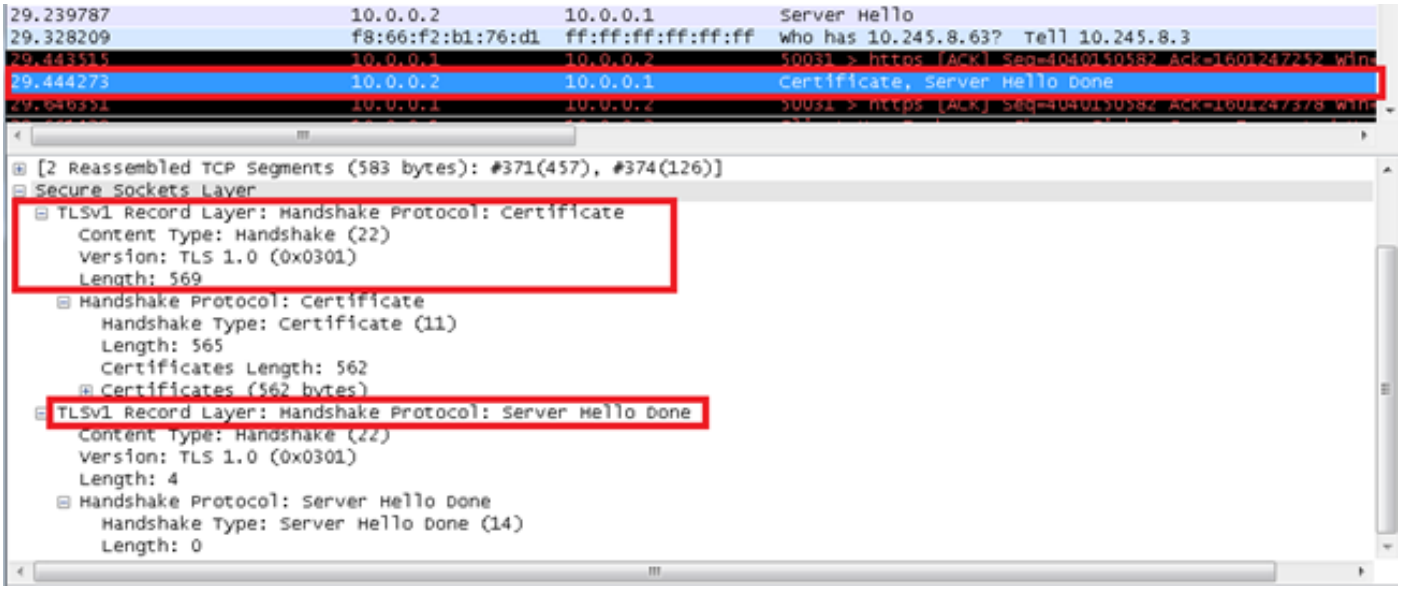


Para las peticiones de la reanudación de la sesión SSL:

- El servidor puede enviar hola una petición al cliente también. Éste es recordar solamente al cliente que debe comenzar la renegociación con una petición de los saludos del cliente cuando es conveniente. El cliente ignora hola la petición del servidor si el proceso del apretón de manos está ya en curso.
- Los mensajes del apretón de manos tienen más precedencia sobre la transmisión de los datos de aplicación. La renegociación debe comenzar en no más que uno o dos veces el tiempo de transmisión de un mensaje de datos de aplicación del Largo máximo.

Saludos del servidor hechos

El mensaje hecho los saludos del servidor es enviado por el servidor para indicar el extremo de los saludos del servidor y de los mensajes asociados. Después de que envíe este mensaje, el servidor espera una respuesta del cliente. Tras el recibo de los saludos del servidor hechos el mensaje, el cliente verifica que el servidor proporcionó a un certificado válido, si procede, y a los controles que los parámetros de los saludos del servidor son aceptables.



Certificado de servidor, intercambio de la clave del servidor, y pedido de certificado (opcional)

- **Certificado de servidor:** Si el servidor se debe autenticar (que es generalmente el caso), el servidor envía su certificado inmediatamente después del mensaje de los saludos del servidor. El tipo de certificado debe ser apropiado para el Key Exchange Algorithm seleccionado de la habitación de la cifra, y es generalmente un certificado X.509.v3.
- **Intercambio de la clave del servidor:** El mensaje de intercambio de la clave del servidor es enviado por el servidor si no tiene ningún certificado. ¿Si el Diffie? Hellman que (DH) los parámetros se incluyen con el certificado de servidor, este mensaje no se utiliza.
- **Pedido de certificado:** Un servidor puede pedir opcionalmente un certificado del cliente, si es apropiado para la habitación seleccionada de la cifra.

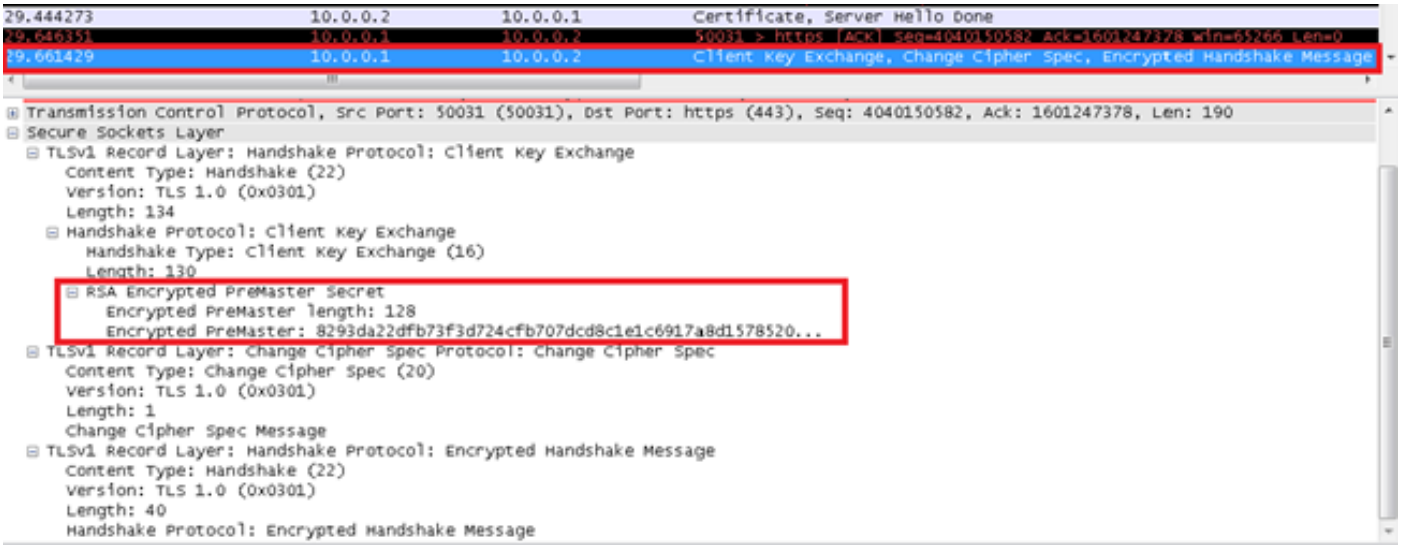
Intercambio del cliente

Certificado del cliente (opcional)

Éste es el primer mensaje que el cliente envía después de que él reciba un mensaje hecho los saludos del servidor. Este mensaje se envía solamente si el servidor pide un certificado. Si no hay certificado conveniente disponible, el cliente envía una alerta del **no_certificate** en lugar de otro. Esta alerta es solamente una advertencia; sin embargo, el servidor pudo responder con una alerta fatal del error del apretón de manos si se requiere la autenticación de cliente. Los Certificados del cliente DH deben hacer juego los parámetros especificados servidor DH.

Intercambio de claves del cliente

El contenido de este mensaje depende del algoritmo de la clave pública seleccionado entre los saludos del cliente y los mensajes de los saludos del servidor. El cliente utiliza una clave del premaster cifrada por el algoritmo del Rivest-Shamir-Addleman (RSA) o el DH para el acuerdo y la autenticación dominantes. Cuando el RSA se utiliza para la autenticación de servidor y el intercambio de claves, un **pre_master_secret** 48-byte es generado por el cliente, cifrado conforme a la clave pública del servidor, y enviado al servidor. El servidor utiliza la clave privada para desencriptar el **pre_master_secret**. Ambas partes entonces convierten el **pre_master_secret** en el **master_secret**.



El certificado verifica (opcional)

Si el cliente envía un certificado con la capacidad de firma, un certificado firmado digitalmente verifica el mensaje se envía para verificar explícitamente el certificado.

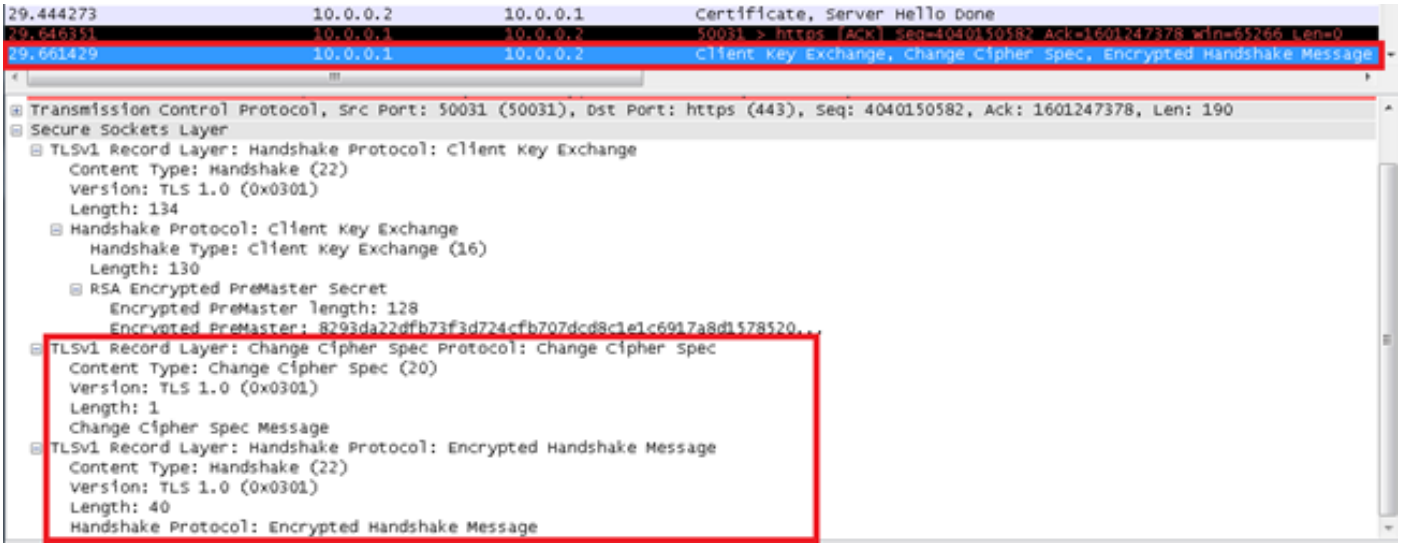
Cambio de la cifra

Cambie los mensajes espec. de la cifra

El mensaje espec. de la cifra del cambio es enviado por el cliente, y el cliente copia espec. pendiente de la cifra (el nuevo) en espec. actual de la cifra (la que fue utilizado previamente). El protocolo espec. de la cifra del cambio existe para las transiciones de señal en las estrategias que cifran. El protocolo consiste en un solo mensaje, que se cifra y se comprime bajo (no espec. actual de la cifra el pendiente). El mensaje es enviado por ambos el cliente y servidor para notificar a la parte receptora que los expedientes subsiguientes están protegidos bajo espec. de la cifra y claves recientemente negociadas. La recepción de este mensaje hace al receptor copiar “leyó hasta que finalice” el estado en “leyó” el estado actual. El cliente envía un intercambio de claves de siguiente del apretón de manos del mensaje espec. de la cifra del cambio y el certificado verifica los mensajes (eventualmente), y el servidor envía uno después de que procese con éxito el mensaje de intercambio de claves que recibió del cliente. Cuando se reanuda una sesión anterior, el mensaje espec. de la cifra del cambio se envía después de los mensajes Hello Messages. En las capturas, el intercambio del cliente, la cifra del cambio, y los mensajes acabados se envían como solo mensaje del cliente.

Mensajes acabados

Un mensaje acabado se envía siempre inmediatamente después que un mensaje espec. de la cifra del cambio para verificar que el intercambio de claves y los procesos de autenticación eran acertados. El mensaje acabado es el primer paquete protegido con los algoritmos, las claves, y los secretos recientemente negociados. No se requiere ningún acuse de recibo del mensaje acabado; los partidos pueden comenzar a enviar los datos encriptados inmediatamente después que envían el mensaje acabado. Los beneficiarios de los mensajes Finished deben verificar que el contenido esté correcto.



Información Relacionada

- [RFC 6101 - El 3.0 de la Versión del protocolo de Secure Sockets Layer]
- [Soporte Técnico y Documentación - Cisco Systems]