Introdução SSL com exemplo de transação e troca de pacotes

Contents

Introduction

Este documento descreve os conceitos básicos do protocolo SSL (Secure Sockets Layer) e fornece um exemplo de transação e captura de pacotes.

Visão geral dos registros SSL

A unidade básica de dados em SSL é um registro. Cada registro consiste em um cabeçalho de registro de cinco bytes, seguido de dados.

Formato de registro

- **Digite:** uint8 - valores listados
- **Versão:** uint16
- **Comprimento:** uint16

Tipo	Versão		Duração	
T	VH	VL	LH	LL

Tipo de registro

Há quatro tipos de registro em SSL:

- **Handshake** (22, 0x16)
- **Modificar especificação do cifrão** (20, 0x14)
- **Alerta** (21, 0x15)
- **Dados do aplicativo** (23, 0x17)

Gravar versão

A versão do registro é um valor de 16 bits e é formatada em ordem de rede.

> **Note**: Para SSL Versão 3 (SSLv3), a versão é 0x0300. Para TLSv1 (Transport Layer Security Version 1), a versão é 0x0301. O Cisco Adaptive Security Appliance (ASA) não oferece suporte a SSL Versão 2 (SSLv2), que usa a versão 0x0002, ou qualquer versão de TLS maior que TLSv1.

Comprimento do registro

O comprimento do registro é um valor de 16 bytes e é formatado em ordem de rede.

Em teoria, isso significa que um único registro pode ter até 65.535 (2^16 -1) bytes de comprimento. O TLSv1 RFC2246 afirma que o comprimento máximo é de 16.383 (2^14 -1) bytes. Sabe-se que os produtos da Microsoft (Microsoft Internet Explorer e Internet Information Services) excedem esses limites.

Tipos de registros

Esta seção descreve os quatro tipos de registros SSL.

Registros de handshake

Os registros de handshake contêm um conjunto de mensagens que são usadas para o handshake. Estas são as mensagens e seus valores:

- **Solicitação Hello** (0, 0x00)
- **Cliente Hello** (1, 0x01)
- **Servidor Hello** (2, 0x02)
- **Certificado** (11, 0x0B)
- **Troca de chaves de servidor** (12, 0x0C)
- **Solicitação de certificado** (13, 0x0D)
- **Servidor concluído** (14, 0x0E)
- **Verificação de certificado** (15, 0x0F)
- **Troca de chave de cliente** (16, 0x10)
- **Concluído** (20, 0x14)

No caso simples, os registros de handshake não são criptografados. No entanto, um registro de handshake que contém uma mensagem concluída é sempre criptografado, pois sempre ocorre após um registro CCS (Change Cipher Spec).

Registros CCS

Os registros CCS são usados para indicar uma alteração em cifras criptográficas. Imediatamente após o registro CCS, todos os dados são criptografados com a nova cifra. Os registros CCS podem ou não ser criptografados; em uma conexão simples com um único handshake, o registro CCS não é criptografado.

Registros de alerta

Os registros de alerta são usados para indicar ao peer que ocorreu uma condição. Alguns alertas são avisos, enquanto outros são fatais e causam falha na conexão. Os alertas podem ou não ser criptografados e podem ocorrer durante um handshake ou durante a transferência de dados. Há dois tipos de alertas:

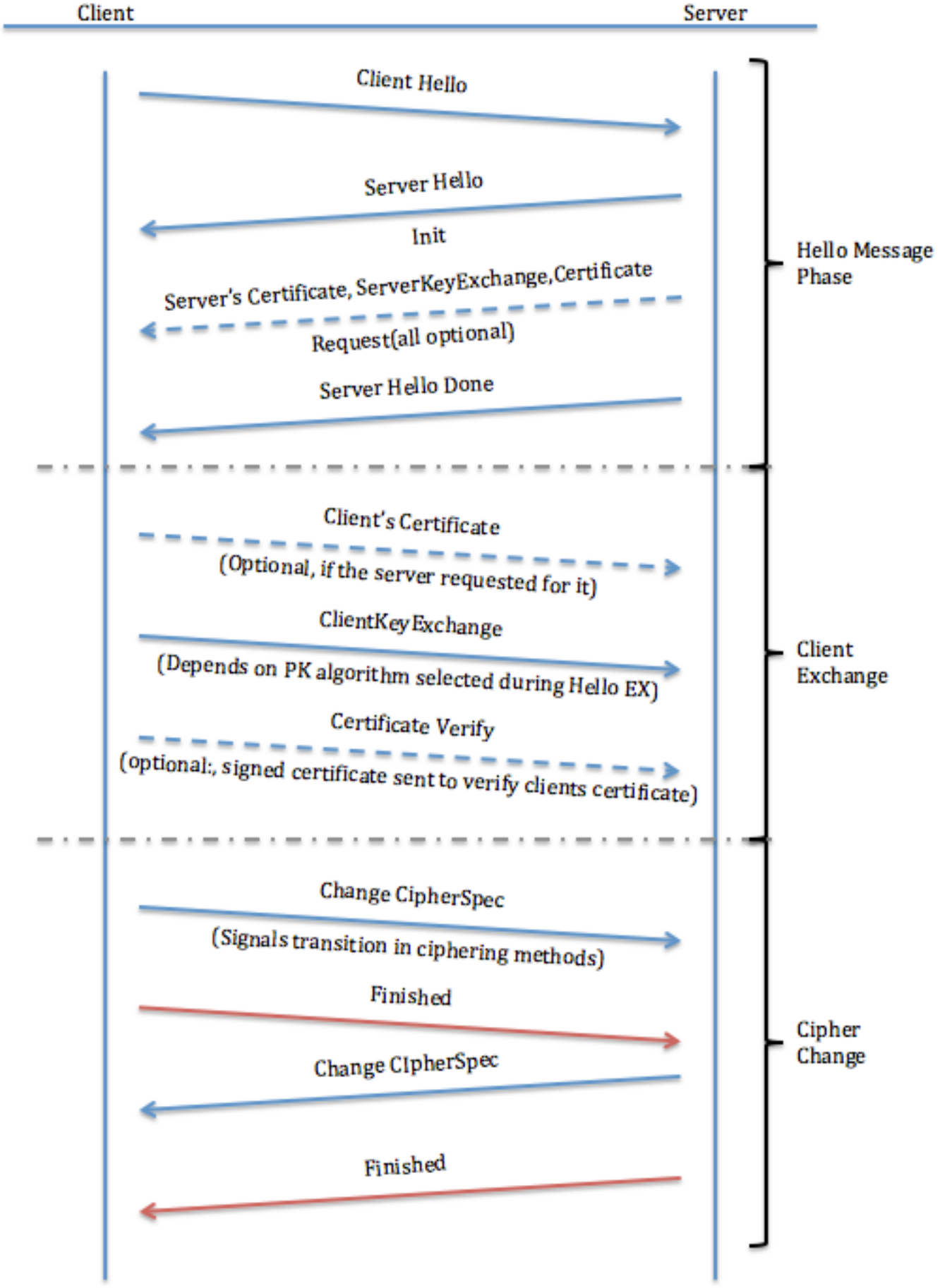
- **Alertas de fechamento:** A conexão entre o cliente e o servidor deve ser fechada corretamente para evitar qualquer tipo de ataque de truncamento. Uma mensagem **close_notify** é enviada indicando ao destinatário que o remetente não enviará mais mensagens nessa conexão.
- **Alertas de erro:** Quando um erro é detectado, a parte detectora envia uma mensagem para a outra parte. Após a transmissão ou o recebimento de uma mensagem de alerta fatal, ambas as partes fecham imediatamente a conexão. Alguns exemplos de alertas de erro são:
  - **inesperada_message** (fatal)
  - **decompression_failure**
  - **handshake_failure**

Registro de dados do aplicativo

Esses registros contêm os dados reais do aplicativo. Essas mensagens são transportadas pela camada de registro e são fragmentadas, comprimidas e criptografadas, com base no estado de conexão atual.

Exemplo de transação

Esta seção descreve um exemplo de transação entre o cliente e o servidor.



O Hello Exchange

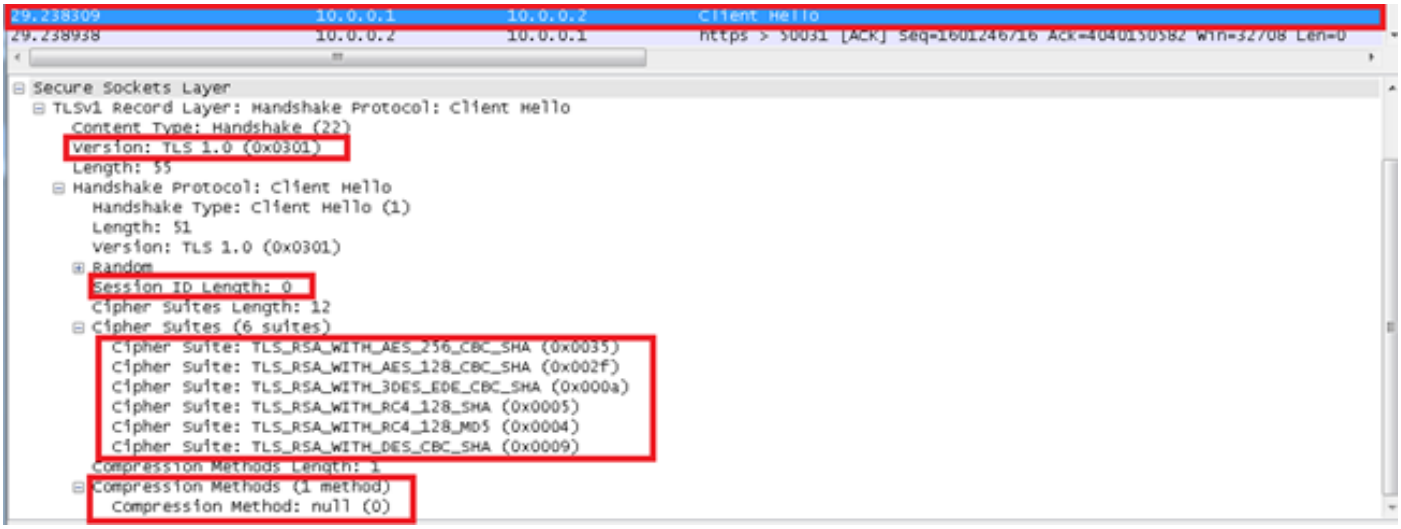
Quando um cliente e um servidor SSL começam a se comunicar, eles concordam em uma versão de protocolo, selecionam algoritmos criptográficos, opcionalmente autentizam um ao outro e usam técnicas de criptografia de chave pública para gerar segredos compartilhados. Esses processos são executados no protocolo handshake. Em resumo, o cliente envia uma mensagem de saudação do cliente ao servidor, que deve responder com uma mensagem de saudação do servidor ou um erro fatal ocorre e a conexão falha. O cliente Hello e o servidor Hello são usados para estabelecer recursos de aprimoramento de segurança entre o cliente e o servidor.

Client Hello

O Cliente Hello envia estes atributos ao servidor:

- **Versão do protocolo:** A versão do protocolo SSL pela qual o cliente deseja se comunicar durante esta sessão.
- **ID da sessão:** A ID de uma sessão que o cliente deseja usar para esta conexão. Na primeira saudação do cliente da troca, a ID da sessão está vazia (consulte a captura de tela do pacote após a anotação).
- **Conjunto de Cifras:** Isso é passado do cliente para o servidor na mensagem de saudação do cliente. Contém as combinações de algoritmos criptográficos suportados pelo cliente na ordem da preferência do cliente (primeira escolha). Cada conjunto de cifras define um algoritmo de troca de chaves e uma especificação de cifra. O servidor seleciona um conjunto de cifras ou, se nenhuma opção aceitável for apresentada, retorna um alerta de falha de handshake e fecha a conexão.
- **Método de compactação:** Inclui uma lista de algoritmos de compressão suportados pelo cliente. Se o servidor não suportar nenhum método enviado pelo cliente, a conexão falhará. O método de compactação também pode ser nulo.

Note: O endereço IP do servidor nas capturas é 10.0.0.2 e o endereço IP do cliente é 10.0.0.1.



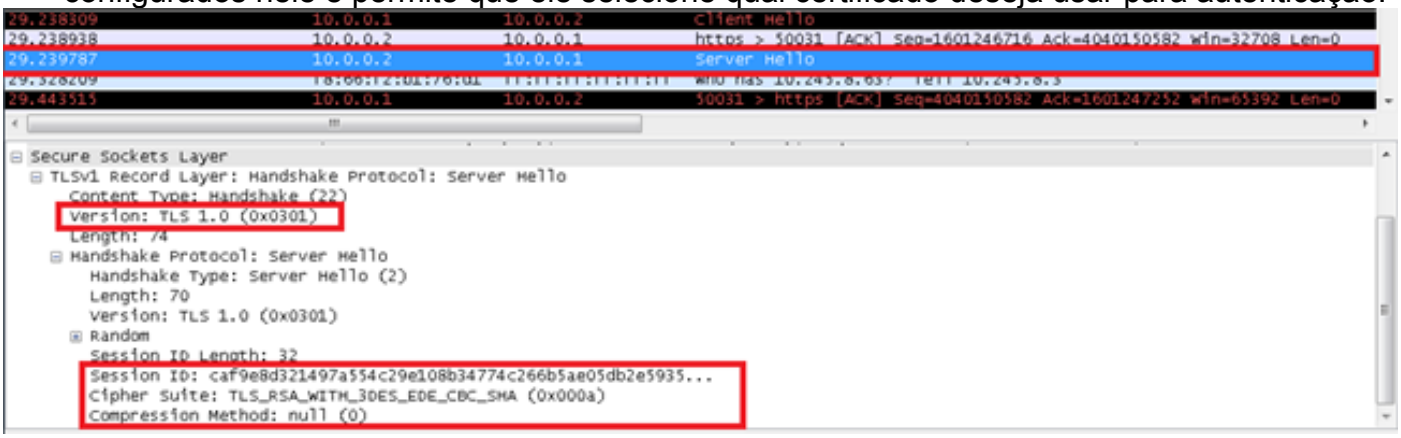
Server Hello

O servidor envia esses atributos de volta ao cliente:

- **Versão do protocolo:** A versão escolhida do protocolo SSL suportada pelo cliente.
- **ID da sessão:** Esta é a identidade da sessão que corresponde a esta conexão. Se a ID da

sessão enviada pelo cliente no Cliente Hello não estiver vazia, o servidor procura uma correspondência no cache da sessão. Se uma correspondência for encontrada e o servidor estiver disposto a estabelecer a nova conexão usando o estado de sessão especificado, o servidor responderá com o mesmo valor fornecido pelo cliente. Isso indica uma sessão retomada e determina que as partes devem prosseguir diretamente para as mensagens concluídas. Caso contrário, este campo contém um valor diferente que identifica a nova sessão. O servidor pode retornar um **session_id** vazio para indicar que a sessão não será armazenada em cache e, portanto, não poderá ser retomada.

- **Conjunto de Cifras:** Conforme selecionado pelo servidor na lista que foi enviada do cliente.
- **Método de compactação:** Conforme selecionado pelo servidor na lista que foi enviada do cliente.
- **Certificate Request:** O servidor envia ao cliente uma lista de todos os certificados configurados nele e permite que ele selecione qual certificado deseja usar para autenticação.

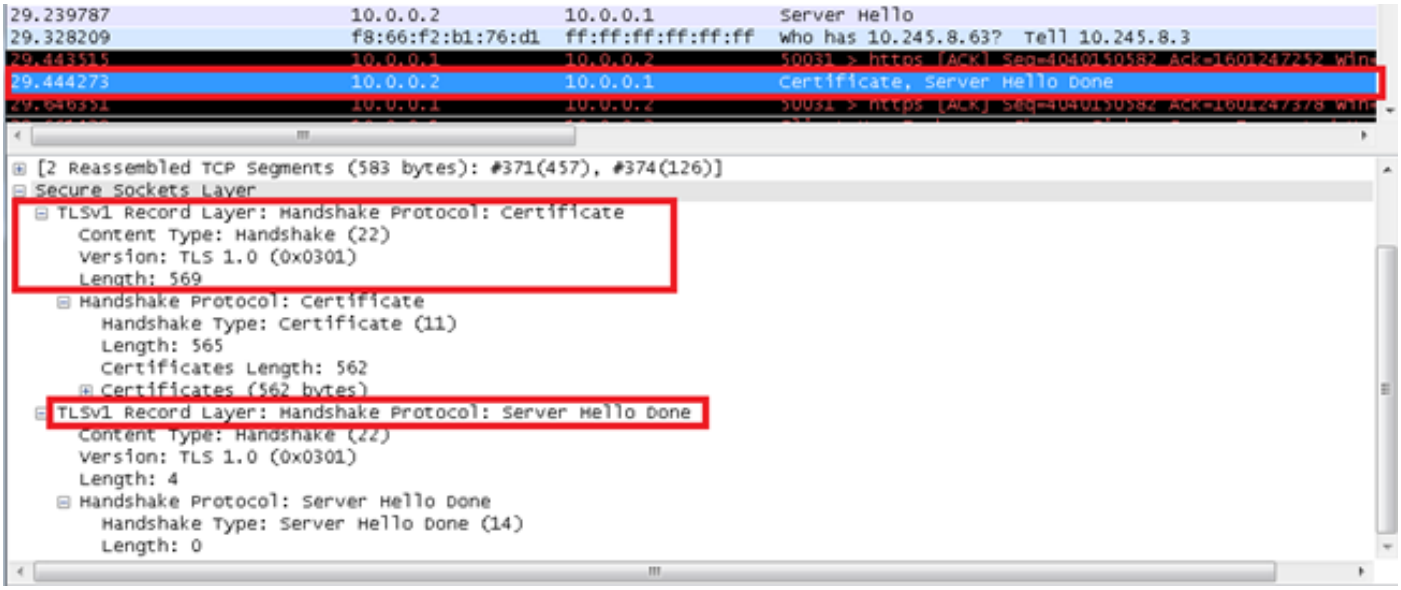


Para solicitações de retomada de sessão SSL:

- O servidor também pode enviar uma solicitação Hello ao cliente. Isso serve apenas para lembrar ao cliente que ele deve iniciar a renegociação com uma solicitação de Hello do cliente quando for conveniente. O cliente ignora a solicitação Hello do servidor se o processo de handshake já estiver em andamento.
- As mensagens de handshake têm mais precedência sobre a transmissão de dados do aplicativo. A renegociação deve começar em uma ou duas vezes o tempo de transmissão de uma mensagem de dados de aplicativo de tamanho máximo.

Servidor Hello concluído

A mensagem de saudação do servidor concluída é enviada pelo servidor para indicar o fim da saudação do servidor e das mensagens associadas. Depois de enviar esta mensagem, o servidor espera uma resposta do cliente. Ao receber a mensagem de saudação do servidor concluída, o cliente verifica se o servidor forneceu um certificado válido, se necessário, e verifica se os parâmetros de saudação do servidor são aceitáveis.



Certificado do servidor, troca de chave do servidor e solicitação de certificado (opcional)

- **Certificado do servidor:** se o servidor precisar ser autenticado (geralmente o caso), o servidor enviará seu certificado imediatamente após a mensagem de saudação do servidor. O tipo de certificado deve ser apropriado para o algoritmo de troca de chave do conjunto de cifras selecionado e é geralmente um certificado X.509.v3.
- **Server Key Exchange:** a mensagem do Server Key Exchange é enviada pelo servidor se ele não tiver certificado. Se os parâmetros Diffie-Hellman(DH) forem incluídos no certificado do servidor, essa mensagem não será usada.
- **Solicitação de certificado:** um servidor pode, opcionalmente, solicitar um certificado do cliente, se apropriado para o conjunto de cifras selecionado.

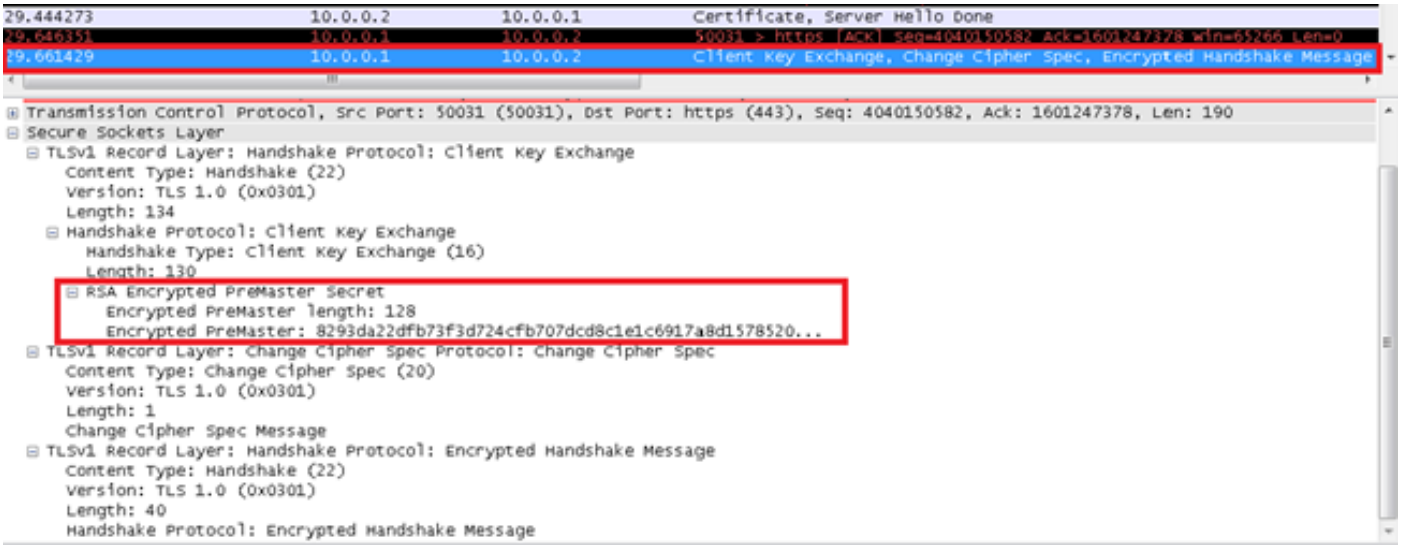
Cliente Exchange

Certificado do cliente (opcional)

Esta é a primeira mensagem que o cliente envia depois de receber uma mensagem de saudação do servidor concluída. Esta mensagem só é enviada se o servidor solicitar um certificado. Se não houver certificado adequado disponível, o cliente envia um alerta **no_certificate**. Esta indicação é apenas uma advertência; no entanto, o servidor pode responder com um alerta de falha fatal do handshake se a autenticação do cliente for necessária. Os certificados DH do cliente devem corresponder aos parâmetros DH especificados pelo servidor.

Chave do cliente

O conteúdo desta mensagem depende do algoritmo de chave pública selecionado entre as mensagens do cliente Hello e do servidor Hello. O cliente usa uma chave pré-master criptografada pelo algoritmo RSA (Rivest-Shamir-Addleman) ou DH (DH) para acordo de chave e autenticação. Quando RSA é usado para autenticação de servidor e troca de chaves, um **pre_master_secret** de 48 bytes é gerado pelo cliente, criptografado sob a chave pública do servidor e enviado ao servidor. O servidor usa a chave privada para descriptografar o **pre_master_secret**. Em seguida, as duas partes convertem o **pre_master_secret** no **master_secret**.



Verificação de certificado (opcional)

Se o cliente enviar um certificado com capacidade de assinatura, uma mensagem de verificação de certificado assinado digitalmente será enviada para verificar explicitamente o certificado.

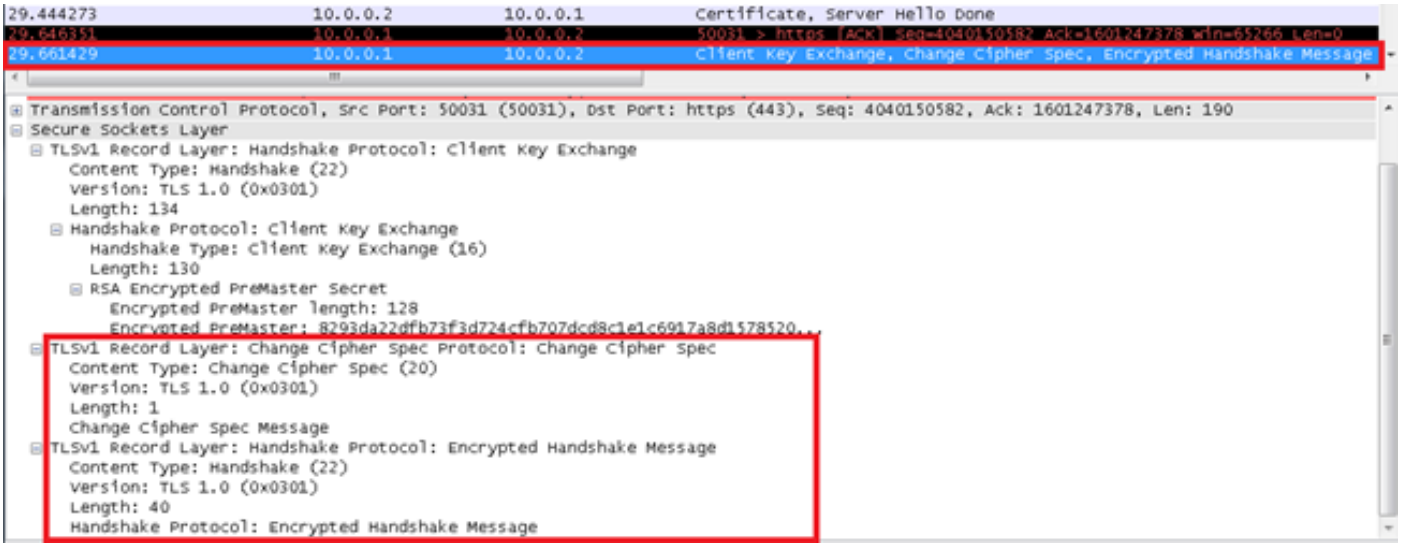
Alteração de cifra

Alterar mensagens das especificações do cliente

A mensagem Change Cipher Spec (Alterar especificação da impressora) é enviada pelo cliente e ele copia a Especificação da Cifra pendente (a nova) na Especificação da Cifra atual (a que foi usada anteriormente). O protocolo Change Cipher Spec existe para sinalizar transições em estratégias de cifragem. O protocolo consiste em uma única mensagem, que é criptografada e compactada sob a especificação de cifra atual (não pendente). A mensagem é enviada pelo cliente e pelo servidor para notificar a parte receptora de que os registros subsequentes estão protegidos sob as chaves e especificações de cifra negociadas mais recentemente. A recepção desta mensagem faz com que o receptor copie o estado de leitura pendente no estado atual de leitura. O cliente envia uma mensagem Change Cipher Spec após as mensagens de troca de chave de handshake e de Verificação de certificado (se houver), e o servidor envia uma mensagem depois de processar com êxito a mensagem de troca de chave recebida do cliente. Quando uma sessão anterior é retomada, a mensagem Change Cipher Spec (Alterar especificação da unidade) é enviada após as mensagens de Hello. Nas capturas, as mensagens Client Exchange, Change Cipher e Finished (Intercâmbio de cliente, Cifra de alteração e Concluído) são enviadas como uma única mensagem do cliente.

Mensagens concluídas

Uma mensagem Finished (Concluído) é sempre enviada imediatamente após uma mensagem Change Cipher Spec (Especificação do editor de alterações) para verificar se os processos de troca de chaves e autenticação foram bem-sucedidos. A mensagem Finished (Concluído) é o primeiro pacote protegido com os algoritmos, chaves e segredos mais recentemente negociados. Nenhuma confirmação da mensagem Finished (Concluído) é necessária; as partes podem começar a enviar dados criptografados imediatamente após enviarem a mensagem Finished (Concluído). Os destinatários das mensagens Concluídas devem verificar se o conteúdo está correto.



Informações Relacionadas

- RFC 6101 - O protocolo SSL versão 3.0
- Wireshark SSL wiki - descriptografar pacotes SSL com o Wireshark
- Suporte Técnico e Documentação - Cisco Systems