Introdução SSL com transação e intercâmbio de pacotes da amostra

Índice

Introdução

Este documento descreve os conceitos básicos do protocolo do secure sockets layer (SSL), e fornece uma transação e uma captura de pacote de informação da amostra.

O SSL grava a vista geral

A unidade básica de dados no SSL é um registro. Cada registro consiste em um encabeçamento de registro do cinco bytes, seguido por dados.

Formato de registro

- Digite: uint8 - valores alistados
- Versão: uint16
- Comprimento: uint16

Tipo	Versão		Duração	
T	VH	VL	LH	LL

Tipo de registro

Há quatro tipos de registro no SSL:

- **Aperto de mão** (22, 0x16)
- **Mude especs. da cifra** (20, 0x14)
- **Alerte** (21, 0x15)
- **Dados do aplicativo** (23, 0x17)

Grave a versão

A versão do registro é um valor 16-byte e é formatada na ordem de rede.

> **Note**: Para a versão de SSL 3 (SSLv3), a versão é 0x0300. Para a versão 1 do Transport Layer Security (TLSv1), a versão é 0x0301. A ferramenta de segurança adaptável de Cisco (ASA) não apoia a versão da versão de SSL 2 (SSLv2), que usa a versão 0x0002, ou algum do TLS maior do que TLSv1.

Comprimento de registro

O comprimento de registro é um valor 16-byte e é formatado na ordem de rede.

Na teoria, isto significa que um único registro pode ser até 65,535 (2^16 -1) bytes de comprimento. O RFC2246 TLSv1 indica que o comprimento máximo é 16,383 (2^14 -1) bytes. Os produtos Microsoft (Microsoft Internet explorer e Internet Information Services) são sabidos para exceder estes limites.

Tipos de registros

Esta seção descreve os quatro tipos de registros SSL.

Registros do aperto de mão

Os registros do aperto de mão contêm um grupo de mensagens que são aperto de mão usado. Estes são as mensagens e seus valores:

- **Olá! pedido** (0, 0x00)
- **Hellos do cliente** (1, 0x01)
- **Servidores hello** (2, 0x02)
- **Certificado** (11, 0x0B)
- **Troca da chave de servidor** (12, 0x0C)
- **Pedido do certificado** (13, 0x0D)
- **Servidores hello feitos** (14, 0x0E)
- **O certificado verifica** (15, 0x0F)
- **Trocas de chave do cliente** (16, 0x10)
- **Terminado** (20, 0x14)

No caso simples, os registros do aperto de mão não são cifrados. Contudo, um registro do aperto de mão que contenha uma mensagem terminada é cifrado sempre, porque ocorre sempre depois que um registro especs. da cifra da mudança (CCS).

Registros CCS

Os registros CCS são usados a fim indicar uma mudança em cifras criptograficamente. Imediatamente depois que o registro CCS, todos os dados é cifrado com a cifra nova. Os registros CCS puderam ou não puderam ser cifrados; em uma conexão simples com um único aperto de mão, o registro CCS não é cifrado.

Registros alertas

Os registros alertas são usados a fim indicar ao par que uma circunstância ocorreu. Alguns alertas são avisos, quando outro forem fatais e fizerem com que a conexão falhe. Os alertas puderam ou não puderam ser cifrados, e puderam ocorrer durante um aperto de mão ou durante transferência de dados. Há dois tipos de alertas:

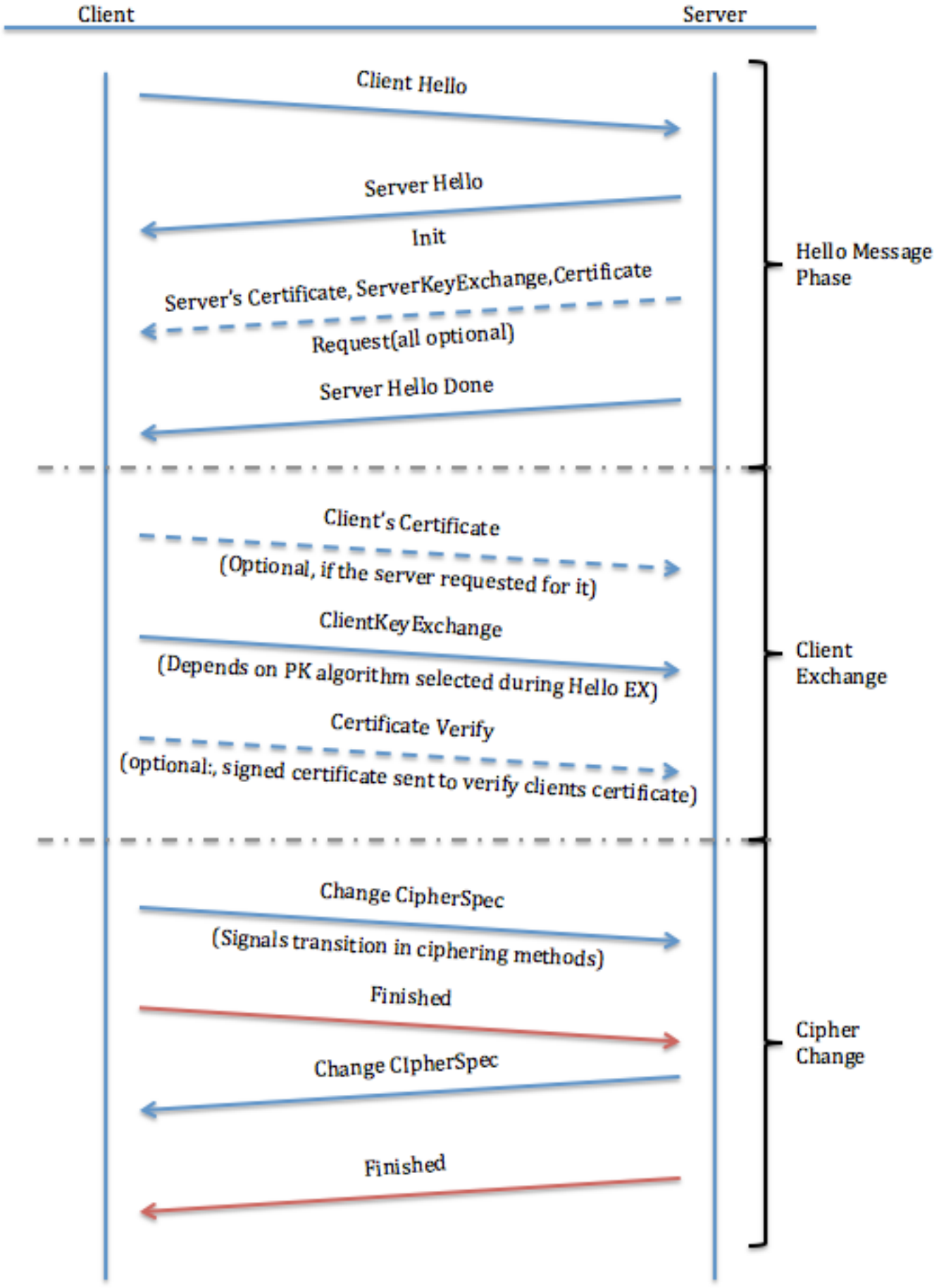
- **Alertas do fechamento:** A conexão entre o cliente e o server deve corretamente ser fechada a fim evitar qualquer tipo de ataques do truncamento. Uma mensagem do **close_notify** é enviada que indique ao receptor que o remetente não enviará anymore mensagens nessa conexão.
- **Alertas do erro:** Quando um erro é detectado, o partido de detecção envia uma mensagem ao outro partido. Em cima da transmissão ou do recibo de um mensagem de alerta fatal, ambos os partidos fecham imediatamente a conexão. Alguns exemplos de alertas do erro são:
  - **unexpected_message** (fatal)
  - **decompression_failure**
  - **handshake_failure**

Registro de dados do aplicativo

Estes registros contêm os dados de aplicativo real. Estas mensagens são levadas pela camada do registro e fragmentadas, comprimidas, e cifradas, com base no estado da conexão atual.

Transação da amostra

Esta seção descreve uma transação da amostra entre o cliente e servidor.



O intercâmbio de hello

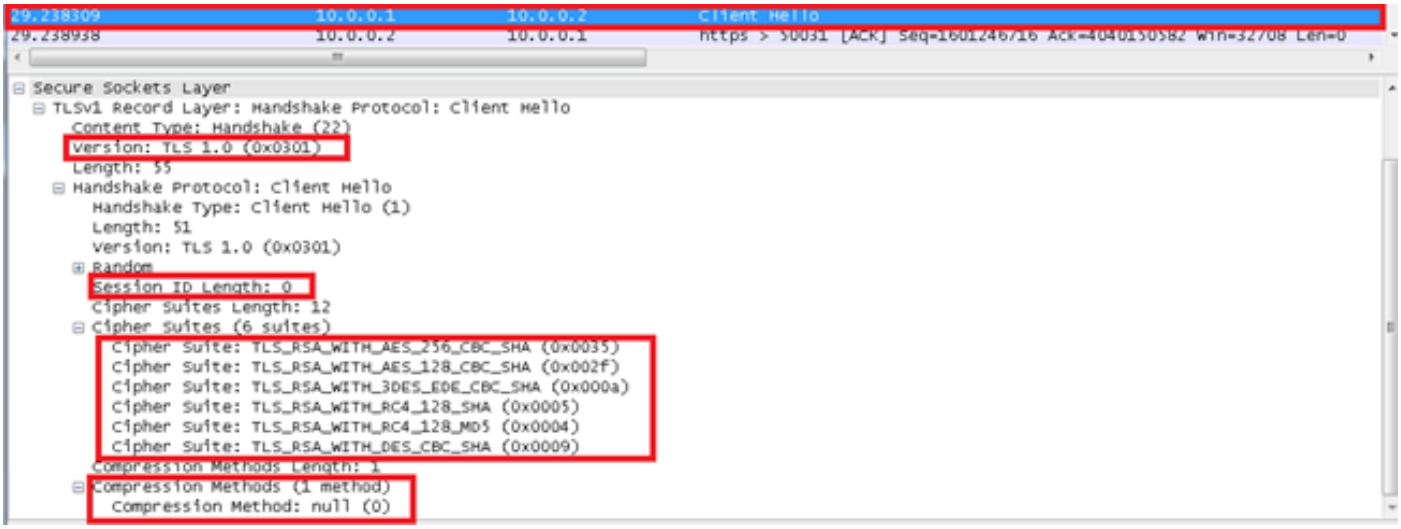
Quando um cliente SSL e um server começam a se comunicar, concorda com uma versão do protocolo, algoritmos criptográficos seletos, autentica-se opcionalmente, e usa-se técnicas da criptografia de chave pública a fim gerar segredos compartilhados. Estes processos são executados no protocolo de handshake. Em resumo, o cliente envia uma mensagem dos hellos do cliente ao server, que deve responder com uma mensagem dos servidores hello ou um erro fatal ocorre e a conexão falha. Os hellos do cliente e os servidores hello são usados para estabelecer capacidades do aprimoramento de segurança entre o cliente e servidor.

Hellos do cliente

O hello do cliente envia estes atributos ao server:

- **Versão do protocolo:** A versão do protocolo SSL por que o cliente deseja se comunicar durante esta sessão.
- **ID de sessão:** O ID de uma sessão os desejos do cliente a usar-se para esta conexão. Nos primeiros hellos do cliente da troca, o ID de sessão está vazio (refira o screen shot da captura de pacote de informação após a nota).
- **Série da cifra:** Isto é passado do cliente ao server na mensagem dos hellos do cliente. Contém as combinações de algoritmos criptográficos apoiados pelo cliente por ordem da preferência do cliente (primeira escolha primeiramente). Cada série da cifra define um Key Exchange Algorithm e umas especs. da cifra. O server seleciona uma série da cifra ou, se nenhuma escolha aceitável é apresentada, retorna um alerta da falha do aperto de mão e fecha a conexão.
- **Método de compactação:** Inclui uma lista de algoritmos de compactação apoiados pelo cliente. Se o server não apoia nenhum método enviado pelo cliente, a conexão falha. O método de compactação pode igualmente ser nulo.

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



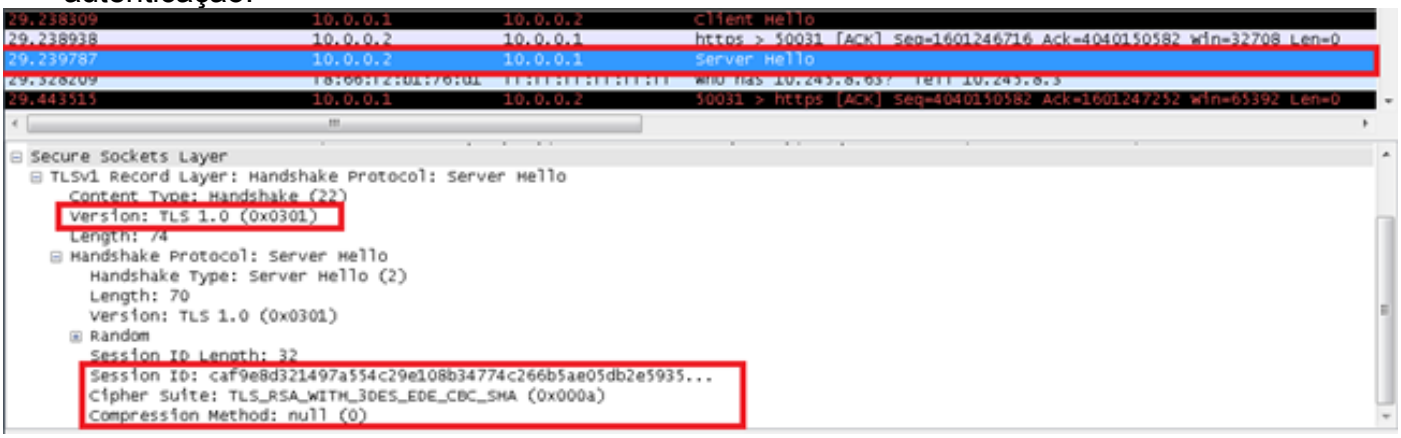
Servidores hello

O server envia para trás estes atributos ao cliente:

- **Versão do protocolo:** A versão escolhida do protocolo SSL que os suportes ao cliente.
- **ID de sessão:** Esta é a identidade da sessão que corresponde a esta conexão. Se o ID de

sessão enviado pelo cliente nos hellos do cliente não está vazio, o server olha no esconderijo da sessão para um fósforo. Se um fósforo é encontrado e o server é disposto estabelecer a nova conexão usando o estado de sessão especificado, o server responde com o mesmo valor que foi fornecido pelo cliente. Isto indica uma sessão recomeçada e dita que os partidos devem continuar diretamente às mensagens terminadas. Se não, este campo contém um valor diferente que identifique a sessão nova. O server pôde retornar um **session_id** vazio a fim indicar que a sessão não estará posta em esconderijo, e não pode consequentemente ser recomeçado.

- **Série da cifra:** Como selecionado pelo server da lista que foi enviada do cliente.
- **Método de compactação:** Como selecionado pelo server da lista que foi enviada do cliente.
- **Pedido do certificado:** O server envia ao cliente uma lista de todos os Certificados que são configurados nela, e permite que o cliente selecione que certificate a querem se usar para a autenticação.

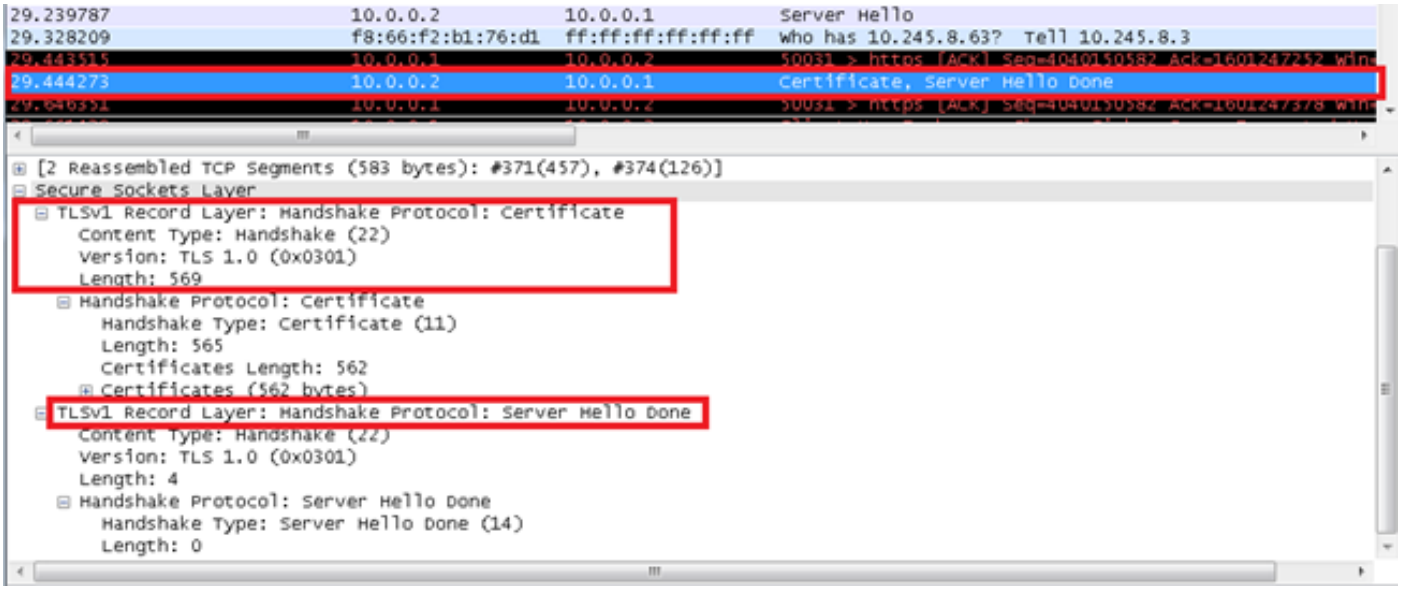


Para pedidos da ressunção da sessão de SSL:

- O server pode enviar olá! um pedido ao cliente também. Esta é lembrar somente o cliente que deve começar a negociação nova com um pedido dos hellos do cliente quando conveniente. O cliente ignora olá! o pedido do server se o processo do aperto de mão é já corrente.
- As mensagens do aperto de mão têm mais precedência sobre a transmissão dos dados do aplicativo. A negociação nova deve começar em não mais de uma ou dois vezes o tempo de transmissão de uma mensagem de dados do aplicativo do comprimento máximo.

Servidores hello feitos

A mensagem feita servidores hello é enviada pelo server a fim indicar a extremidade dos servidores hello e das mensagens associadas. Depois que envia esta mensagem, o server espera uma resposta do cliente. Após recepção dos servidores hello feitos a mensagem, o cliente verifica que o server forneceu um certificado válido, se for necessário, e certifica-se dos parâmetros dos servidores hello sejam aceitáveis.



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

- **Certificado de servidor:** Se o server deve ser autenticado (que é geralmente o caso), o server envia seu certificado imediatamente depois da mensagem dos servidores hello. O tipo do certificado deve ser apropriado para o Key Exchange Algorithm selecionado da série da cifra, e é geralmente um certificado X.509.v3.
- **Troca da chave de servidor:** O mensagem de intercâmbio da chave de servidor está enviado pelo server se não tem nenhum certificado. Se os parâmetros do Diffie-Hellman (DH) são incluídos com o certificado de servidor, esta mensagem não está usada.
- **Pedido do certificado:** Um server pode opcionalmente pedir um certificado do cliente, se apropriado para a série selecionada da cifra.

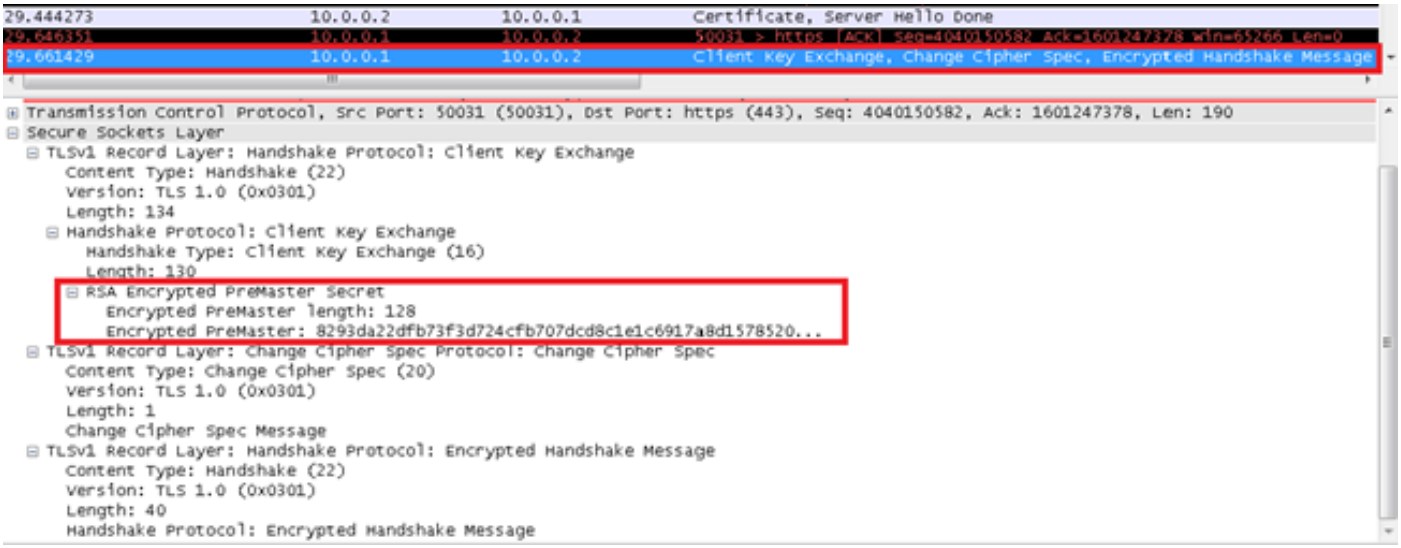
Troca do cliente

Certificado de cliente (opcional)

Esta é a primeira mensagem que o cliente envia depois que recebe uma mensagem feita servidores hello. Esta mensagem é enviada somente se o server pede um certificado. Se nenhum certificado apropriado está disponível, o cliente envia um alerta do **no_certificate** pelo contrário. Este alerta é somente um aviso; contudo, o server pôde responder com um alerta fatal da falha do aperto de mão se a authenticação do cliente é exigida. Os Certificados do cliente DH devem combinar os parâmetros especificados server DH.

Trocas de chave do cliente

O índice desta mensagem depende do algoritmo da chave pública selecionado entre os hellos do cliente e as mensagens dos servidores hello. O cliente usa uma chave do premaster cifrada pelo algoritmo de Rivest-Shamir-Addleman (RSA) ou o DH para o acordo e a autenticação chaves. Quando o RSA é usado para a autenticação de servidor e as trocas de chave, um **pre_master_secret** 48-byte está gerado pelo cliente, cifrado sob a chave pública do server, e enviado ao server. O server usa a chave privada a fim decifrar o **pre_master_secret**. Ambos os partidos convertem então o **pre_master_secret no master_secret**.



O certificado verifica (opcional)

Se o cliente envia um certificado com capacidade de assinatura, um certificado digitalmente-assinado verifica que a mensagem está enviada a fim verificar explicitamente o certificado.

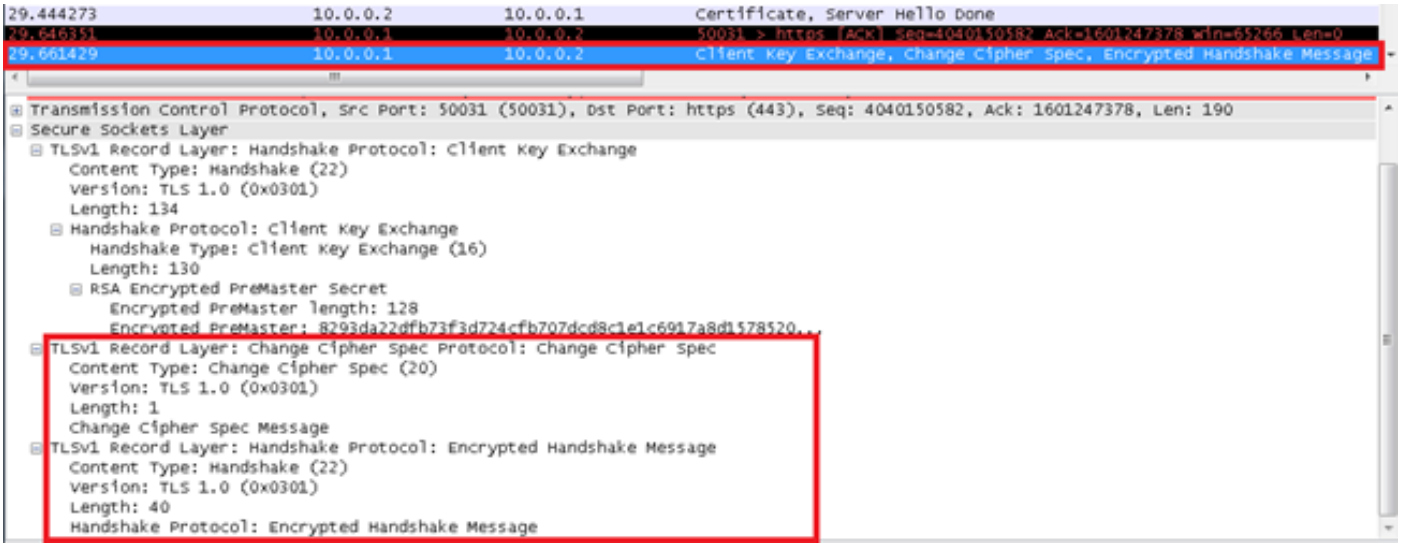
Mudança da cifra

Mude mensagens especs. da cifra

A mensagem especs. da cifra da mudança é enviada pelo cliente, e o cliente copia as especs. pendentes da cifra (o novo) nas especs. atuais da cifra (essa que foi usada previamente). O protocolo especs. da cifra da mudança existe transições de sinal em estratégias de cálculo. O protocolo consiste em uma única mensagem, que seja cifrada e comprimida sob (não as especs. atuais da cifra o pendente). A mensagem é enviada por ambos o cliente e servidor a fim notificar a parte de recebimento que os registros subsequentes estão protegidos sob as especs. da cifra e as chaves recentemente negociadas. A recepção desta mensagem faz com que o receptor copie lida durante o estado no estado atual lido. O cliente envia uma mensagem especs. da cifra da mudança após as trocas de chave do aperto de mão e o certificado verifica mensagens (eventualmente), e o server envia um depois que processa com sucesso a mensagem que de trocas de chave recebeu do cliente. Quando uma sessão precedente é recomeçada, a mensagem especs. da cifra da mudança está enviada após os mensagens Hello Messages. Nas captações, a troca do cliente, a cifra da mudança, e as mensagens terminadas são enviadas como uma única mensagem do cliente.

Mensagens terminadas

Uma mensagem terminada é enviada sempre imediatamente depois que uma mensagem especs. da cifra da mudança a fim verificar que as trocas de chave e os processos de autenticação eram bem sucedidos. A mensagem terminada é o primeiro pacote protegido com os algoritmos, as chaves, e os segredos recentemente negociados. Nenhum reconhecimento da mensagem terminada é exigido; os partidos podem começar a enviar dados criptografados imediatamente depois que enviam a mensagem terminada. Os receptores de mensagens Finished devem verificar que os índices estão corretos.



Informações Relacionadas

- RFC 6101 - O 3.0 da versão do protocolo do secure sockets layer
- Wiki de Wireshark SSL - decifre pacotes SSL com Wireshark
- Suporte Técnico e Documentação - Cisco Systems