帶有示例交易和資料包交換的SSL簡介

目錄

簡介

本文檔介紹安全套接字層(SSL)協定的基本概念，並提供一個事務和資料包捕獲示例。

SSL記錄概述

SSL中的基本資料單位是記錄。每個記錄都包含一個5位元組的記錄報頭，後跟資料。

記錄格式

- **Type:**uint8 — 列出的值
- **版本:**uint16
- **長度**:uint16

類型	版本		長度	
T	VH	VL	LH	LL

記錄型別

SSL中有四種記錄型別：

- **握**手(22, 0x16)
- **更改密碼**規格(20、0x14)
- **警**報(21, 0x15)
- **應用程**序資料(23、0x17)

記錄版本

記錄版本是16位值，按網路順序格式化。

> **附註**：對於SSL版本3(SSLv3)，版本為0x0300。對於傳輸層安全版本1(TLSv1)，版本為0x0301。思科自適應安全裝置(ASA)不支援使用版本0x002的SSL版本2(SSLv2)或大於TLSv1的任何版本的TLS。

記錄長度

記錄長度是一個16位元組的值，並按網路順序格式化。

理論上，這意味著單個記錄的長度可以高達65,535(2^16 -1)位元組。TLSv1 RFC2246宣告最大長度為16,383(2^14 -1)位元組。眾所周知，Microsoft產品（Microsoft Internet Explorer和Internet Information Services）超出了這些限制。

記錄型別

本節介紹四種型別的SSL記錄。

握手記錄

握手記錄包含一組用於握手的消息。以下是訊息及其價值：

- **Hello請**求(0, 0x00)
- **客戶端**Hello(1, 0x01)
- **伺服器**Hello(2, 0x02)
- **證**書(11, 0x0B)
- **伺服器密**鑰交換(12, 0x0C)
- **證書**請求(13, 0x0D)
- **伺服器Hello**完成(14, 0x0E)
- **證書驗**證(15, 0x0F)
- **客戶端密**鑰交換(16, 0x10)
- **已**完成(20, 0x14)

在簡單情況下，握手記錄不會加密。但是，包含完成消息的握手記錄總是加密的，因為它總是出現在更改密碼規範(CCS)記錄之後。

CCS記錄

CCS記錄用於指示加密密碼的變化。在CCS記錄之後，立即使用新密碼加密所有資料。CCS記錄可能加密，也可能不加密；在使用一次握手的簡單連線中，CCS記錄不會加密。

警報記錄

警報記錄用於指示對等體發生了情況。某些警報是警告，而其它警報是致命的並會導致連線失敗。警報可能已被加密，也可能未被加密，並且可能發生在握手或資料傳輸期間。有兩種型別的警報：

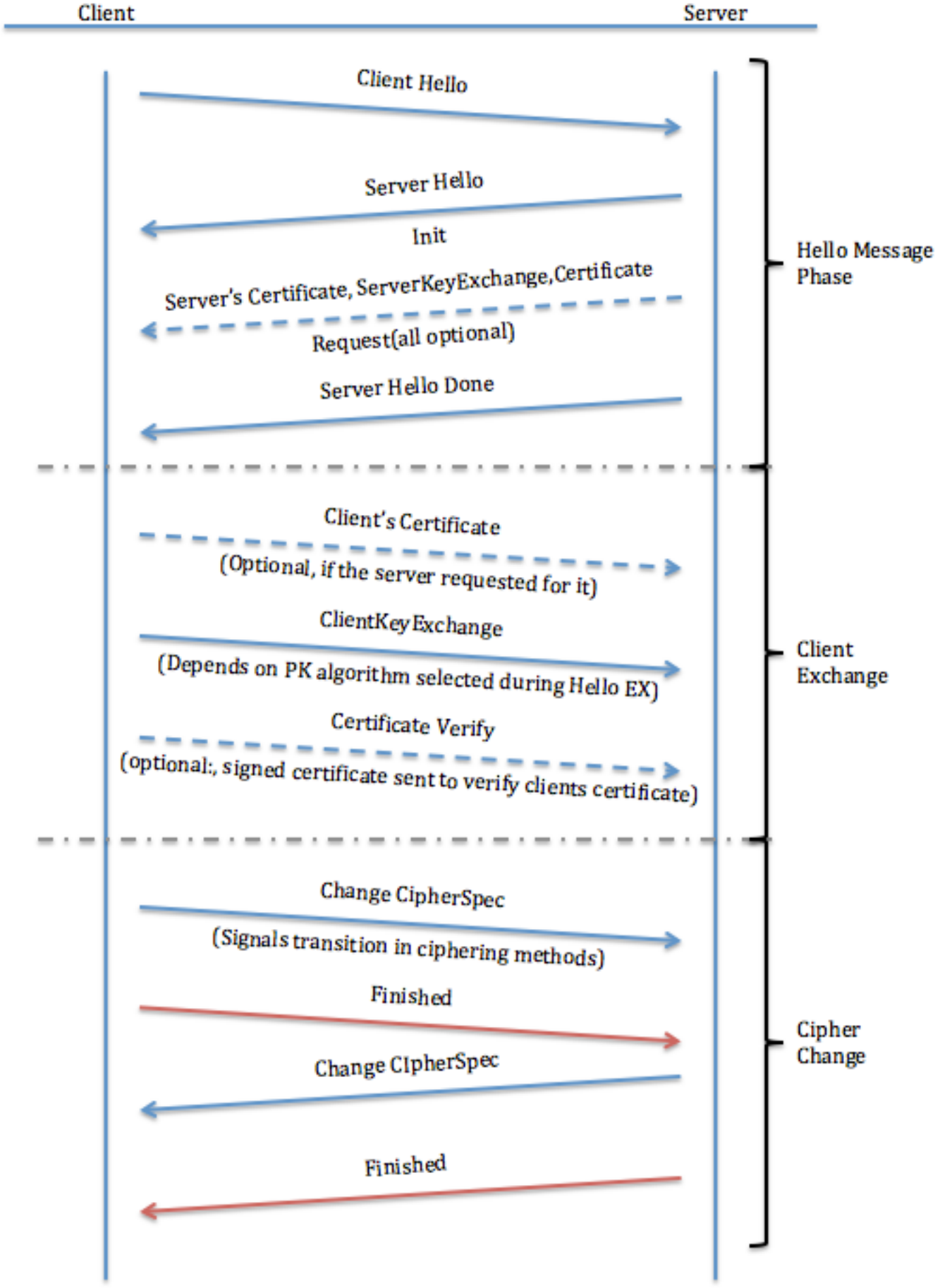
- **關閉警報**：必須正確關閉客戶端與伺服器之間的連線，以避免任何型別的截斷攻擊。傳送一則close_notify消息，向收件人指示發件人將不會在該連線上傳送其他消息。
- **錯誤警報**：檢測到錯誤時，檢測方會向對方傳送消息。在傳輸或收到致命警報消息後，雙方立即關閉連線。錯誤警報的一些示例包括：
  - unexpected_message（致命）
  - expression_failure
  - handshake_failure

應用程式資料記錄

這些記錄包含實際的應用程式資料。這些消息由記錄層承載，並根據當前連線狀態進行分段、壓縮和加密。

事務處理示例

本節介紹客戶端和伺服器之間的事務示例。



Hello Exchange

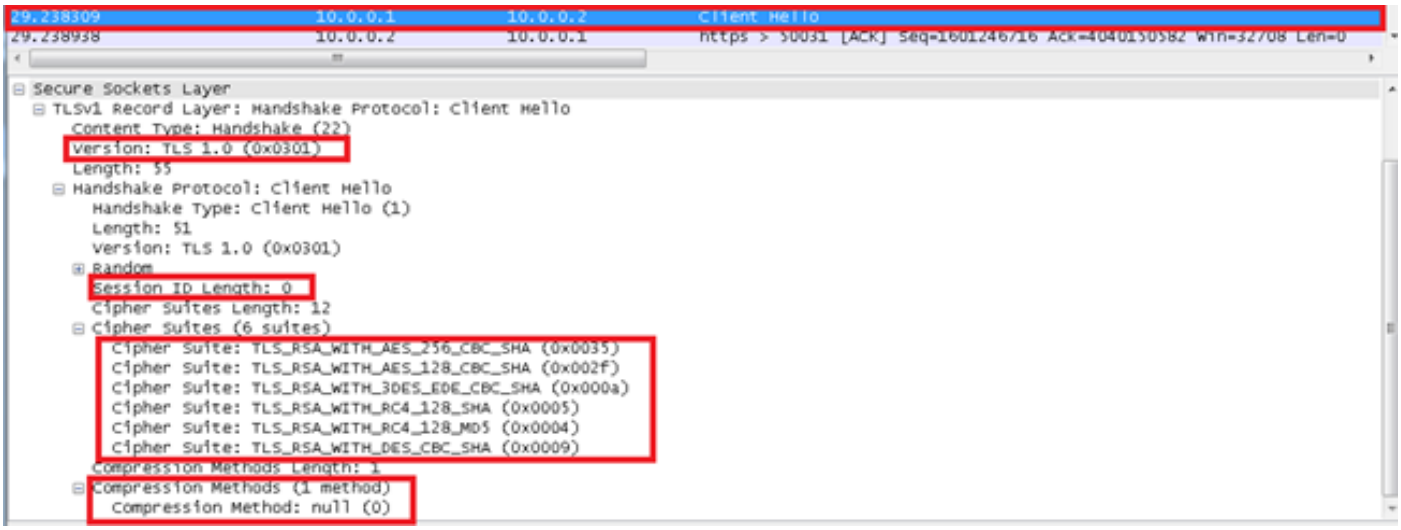
當SSL客戶端和伺服器開始通訊時，它們就協定版本達成一致、選擇加密演算法、可選地相互進行身份驗證，並使用公開金鑰加密技術來生成共用金鑰。這些過程在握手協定中執行。總而言之，客戶端向伺服器傳送客戶端Hello消息，伺服器必須響應伺服器Hello消息或發生致命錯誤並且連線失敗。客戶端Hello和伺服器Hello用於在客戶端和伺服器之間建立安全增強功能。

客戶端Hello

客戶端Hello將以下屬性傳送到伺服器：

- **協定版本**：客戶端希望在此會話期間通訊的SSL協定的版本。
- **會話ID:**客戶端希望用於此連線的會話的ID。在交換器的第一個Client Hello中，會話ID為空（請參閱註釋之後的資料包捕獲螢幕截圖）。
- **密碼套件**：在Client Hello消息中將此消息從客戶端傳遞到伺服器。它包含客戶端支援的加密演算法的組合，按客戶端的優先順序（首選優先）。 每個密碼套件都定義了金鑰交換演算法和密碼規範。伺服器選擇密碼套件，或者，如果沒有提供可接受的選項，則返回握手失敗警報並關閉連線。
- **壓縮方法**：包括客戶端支援的壓縮演算法清單。如果伺服器不支援客戶端傳送的任何方法，則連線失敗。壓縮方法也可以為空。

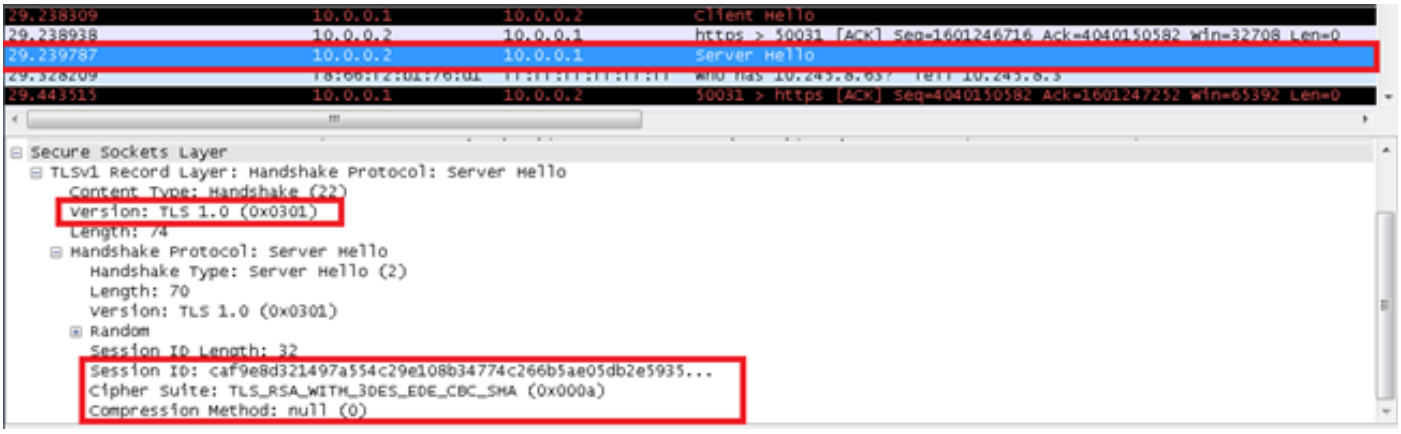
附註：捕獲中的伺服器IP地址為10.0.0.2，客戶端IP地址為10.0.0.1。



伺服器Hello

伺服器會將這些屬性傳送回使用者端：

- **協定版本**：客戶端支援的SSL協定的所選版本。
- **會話ID:**這是與此連線對應的會話標識。如果客戶端在Client Hello中傳送的會話ID不為空，伺服器將在會話快取中查詢匹配項。如果找到匹配項，並且伺服器願意使用指定的會話狀態建立新連線，則伺服器將使用客戶端提供的相同值進行響應。這表示已恢復會話，並指示各方必須直接處理已完成的消息。否則，此欄位包含用於標識新會話的不同值。伺服器可能返回空的session_id，以指示將不快取該會話，因此無法恢復該會話。
- **密碼套件**：由伺服器從從客戶端傳送的清單中選擇的。
- **壓縮方法**：由伺服器從從客戶端傳送的清單中選擇的。
- **證書請求**：伺服器會傳送給使用者端一個清單，列出其上設定的所有憑證，並允許使用者端選擇您要用來進行驗證的憑證。

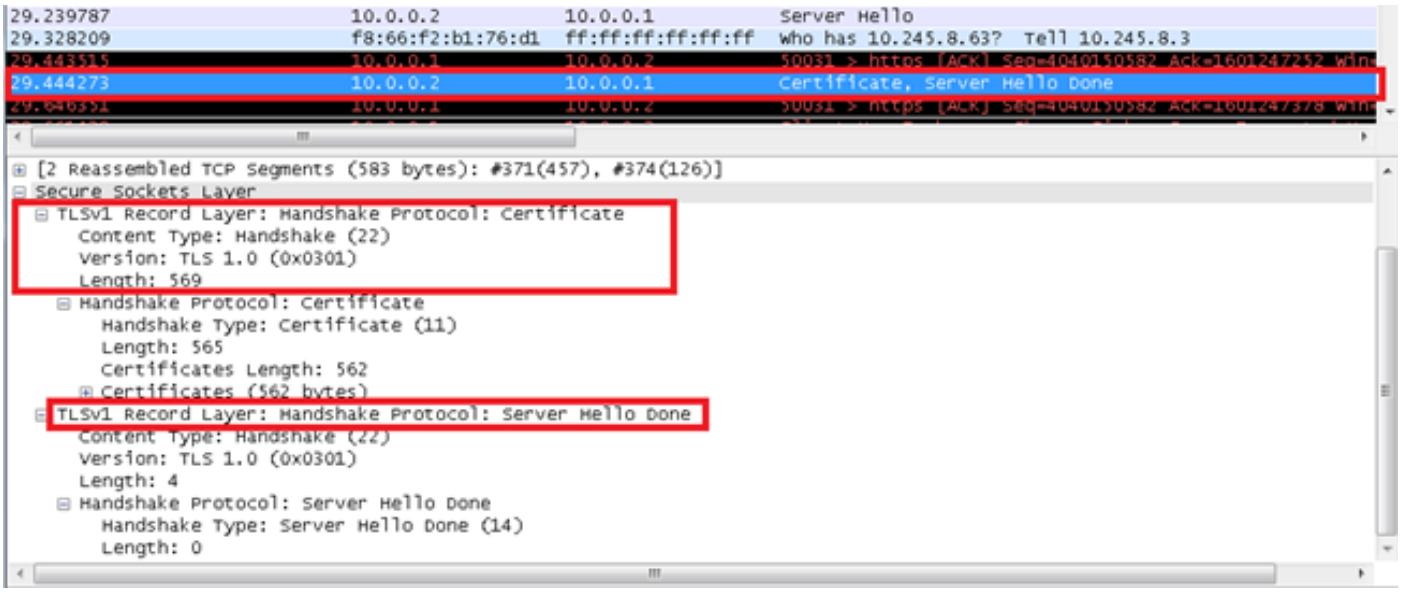


對於SSL會話恢復請求：

- 伺服器也可以向客戶端傳送Hello請求。這只是提醒客戶端，在方便時，應該使用客戶端Hello請求開始重新協商。如果握手過程已在進行，客戶端將忽略來自伺服器的Hello請求。
- 握手消息的優先順序高於應用資料的傳輸。重新協商開始的時間不得超過最大長度應用資料消息的傳輸時間的一倍或兩倍。

伺服器Hello完成

伺服器傳送Hello Done消息以指示伺服器問候的結束和相關消息。在傳送此消息後，伺服器會等待客戶端響應。收到伺服器Hello Done消息後，客戶端驗證伺服器是否提供了有效的證書（如果需要），並檢查伺服器Hello引數是否可接受。



伺服器證書、伺服器金鑰交換和證書請求（可選）

- **伺服器證書**：如果伺服器必須經過身份驗證（通常情況下），則伺服器會在伺服器問候消息後立即傳送其證書。證書型別必須適用於所選密碼套件金鑰交換演算法，並且通常是X.509.v3證書。
- **伺服器金鑰交**換：如果伺服器沒有證書，則伺服器會傳送伺服器金鑰交換消息。如果伺服器憑證中包含Diffie-Hellman(DH)引數，則不使用此訊息。
- **證書請求**：如果適用於所選密碼套件，伺服器可以選擇從客戶端請求證書。

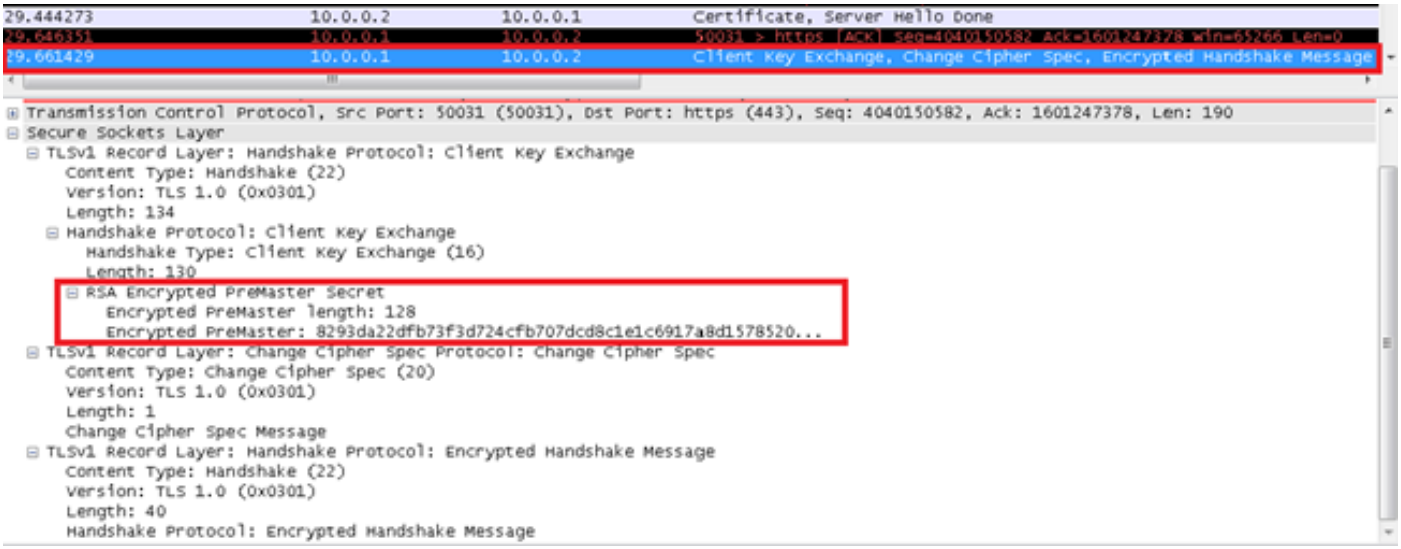
客戶端交換

客戶端證書（可選）

這是客戶端在收到伺服器Hello Done消息後傳送的第一個消息。僅當伺服器請求證書時才傳送此消息。如果沒有合適的證書可用，則客戶端將傳送**no_certificate**警報。此警報只是警告；但是，如果需要客戶端身份驗證，伺服器可能會發出致命握手失敗警報來響應。客戶端DH證書必須與伺服器指定的DH引數匹配。

客戶端金鑰交換

此消息的內容取決於在客戶端Hello消息和伺服器Hello消息之間選擇的公鑰演算法。客戶端使用Rivest-Shamir-Addleman(RSA)演算法加密的預主金鑰，或DH進行金鑰協定和身份驗證。將RSA用於伺服器身份驗證和金鑰交換時，客戶端將生成48位元組的**pre_master_secret**，在伺服器公共金鑰下加密並傳送到伺服器。伺服器使用私鑰對**pre_master_secret進行解密**。然後，雙方將**pre_master_secret**轉換為**master_secret**。



證書驗證（可選）

如果使用者端傳送一個具有簽署功能的憑證，會傳送一則數位簽名的憑證驗證訊息，以便明確驗證憑證。

密碼更改

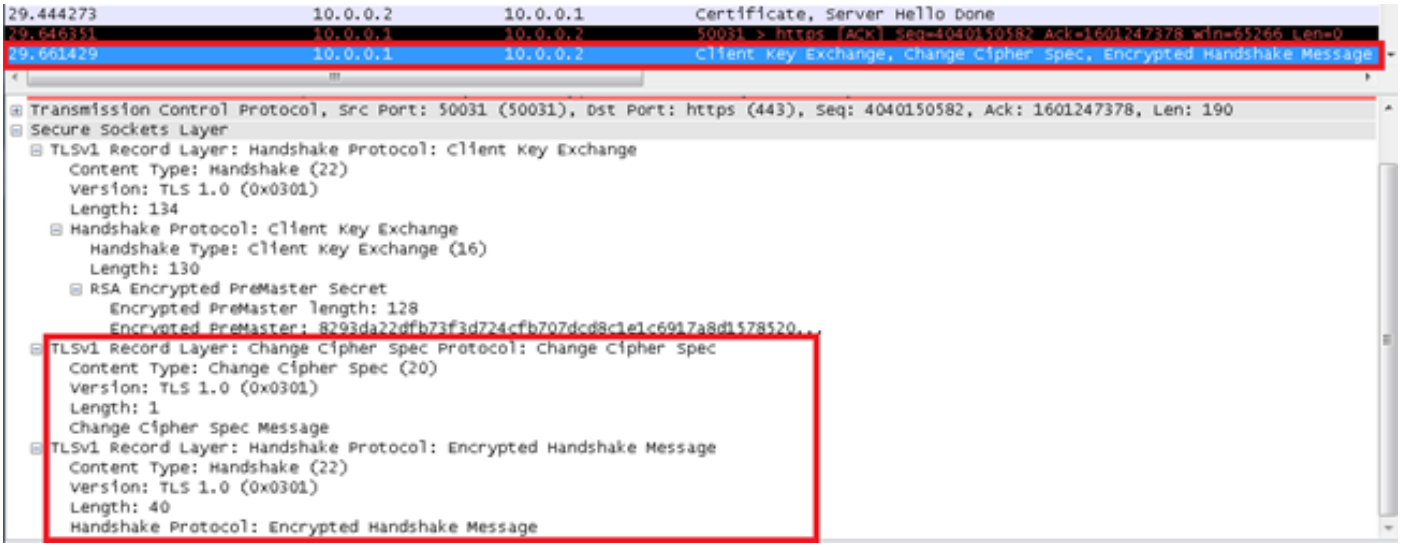
更改密碼規範消息

「更改密碼規範」消息由客戶端傳送，客戶端將待處理的密碼規範（新的密碼規範）複製到當前密碼規範（以前使用的密碼規範）中。 更改密碼規範協定存在於密碼策略中，用於發出轉換信號。該協定由單個消息組成，該消息在當前（不是待定）密碼規範下加密和壓縮。客戶端和伺服器均傳送該消息，以通知接收方，後續記錄受最近協商的密碼規範和金鑰的保護。接收該消息會導致接收方將讀取的掛起狀態複製到讀取的當前狀態。在握手金鑰交換和證書驗證消息（如果有）之後，客戶端傳送「更改密碼規範」消息，伺服器在成功處理從客戶端接收的金鑰交換消息之後傳送一則消息。當上一會話恢復時，「更改密碼規範」消息在Hello消息之後傳送。在捕獲中，「客戶端交換」、「更改密碼」和「完成」消息作為單個消息從客戶端傳送。

已完成消息

始終在「更改密碼規範」消息之後立即傳送「已完成」消息，以驗證金鑰交換和身份驗證過程是否成功。Finished消息是具有最近協商的演算法、金鑰和機密的第一個受保護資料包。不需要確認Finished消息；傳送完成消息後，各方可以立即開始傳送加密資料。已完成郵件的收件人必須驗證

內容是否正確。



相關資訊

- [RFC 6101 — 安全套接字層協定版本3.0]
- [Wireshark SSL wiki -]使用Wireshark解密SSL資料包
- [技術支援與文件 - Cisco Systems]