SSL简介与示例事务和数据包交换

目录

简介

本文档介绍安全套接字层(SSL)协议的基本概念，并提供一个事务和数据包捕获示例。

SSL记录概述

SSL中的基本数据单位是记录。每条记录都包含一个五字节的记录报头，后跟数据。

记录格式

- **type**：uint8 — 列出的值
- **版本**:uint16
- **篇幅**：uint16

类型	version		长度	
T	VH	VL	LH	LL

记录类型

SSL中有四种记录类型：

- **握手**(22, 0x16)
- **更改密码规**范(20, 0x14)
- **警**报(21, 0x15)
- **应用程**序数据(23, 0x17)

记录版本

记录版本是16位值，按网络顺序格式化。

> **注意**：对于SSL版本3(SSLv3)，版本为0x0300。对于传输层安全版本1(TLSv1)，版本为0x0301。思科自适应安全设备(ASA)不支持使用的SSL版本2(SSLv2)版本0x0002，或任何TLS版本大于TLSv1。

记录长度

记录长度为16字节值，按网络顺序格式化。

理论上，这意味着单个记录的长度最多可达65,535(2^16 -1)字节。TLSv1 RFC2246规定最大长度为16,383(2^14 -1)字节。Microsoft产品（Microsoft Internet Explorer和Internet信息服务）已知超出这些限制。

记录类型

本节介绍四种SSL记录类型。

握手记录

握手记录包含用于握手的一组消息。以下是消息及其值：

- **Hello请**求(0, 0x00)
- **客户端**Hello(1, 0x01)
- **服务器**Hello(2, 0x02)
- **证**书(11, 0x0B)
- **服务器密钥**交换(12, 0x0C)
- **证书请**求(13, 0x0D)
- **服务器Hello完**成(14, 0x0E)
- **证书验**证(15, 0x0F)
- **客户端密**钥交换(16, 0x10)
- **完**成(20, 0x14)

在简单情况下，握手记录不加密。但是，包含完成消息的握手记录始终会加密，因为它始终发生在更改密码规范(CCS)记录之后。

CCS记录

使用CCS记录来指示密码的变化。在CCS记录后，所有数据都使用新密码加密。CCS记录可能被加密，也可能不被加密；在与一次握手的简单连接中，CCS记录不会加密。

警报记录

警报记录用于向对等体指示已发生情况。某些警报是警告，而其他警报是致命的，导致连接失败。警报可能已加密，也可能未加密，可能在握手期间或数据传输期间发生。警报分为两种类型：

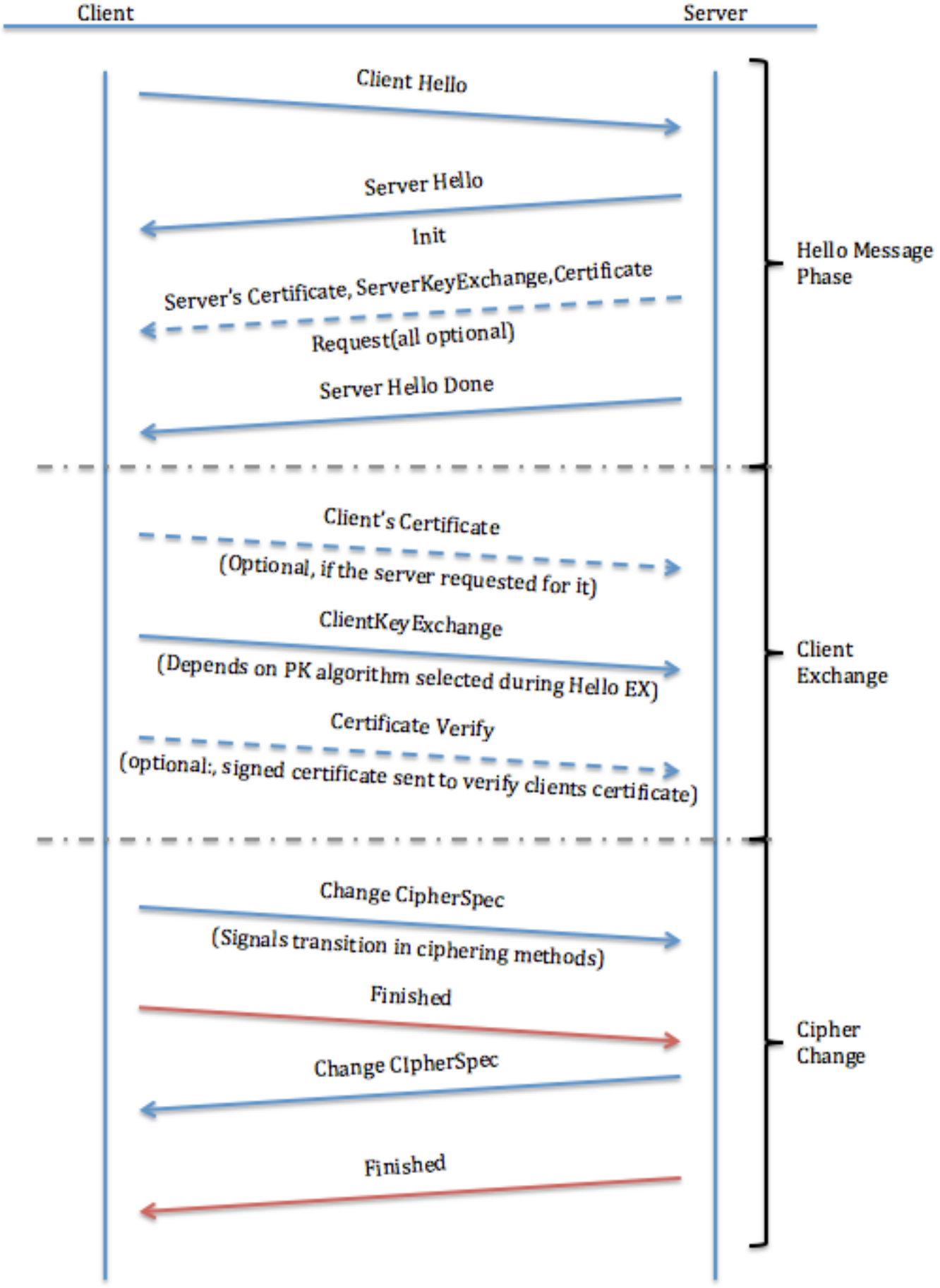
- **关闭警报**：客户端和服务器之间的连接必须正确关闭，以避免任何类型的截断攻击。将发**送一封**close_notify消息，该消息指示发送方不再在该连接上发送邮件。
- **错误警报**：当检测到错误时，检测方向另一方发送消息。在发送或接收致命警报消息时，双方立即关闭连接。错误警报的一些示例包括：
  - **意外消息**（致命）
  - decomplation_failure
  - **握手失败**

应用数据记录

这些记录包含实际应用数据。这些消息由记录层承载，并根据当前连接状态进行分片、压缩和加密。

交易示例

本节介绍客户端和服务器之间的示例事务。


Client
Server
Client Hello
Server Hello
Init
Server's Certificate, ServerKeyExchange,Certificate
Request(all optional)
Server Hello Done
Hello Message Phase
Client's Certificate
(Optional, if the server requested for it)
ClientKeyExchange
(Depends on PK algorithm selected during Hello EX)
Certificate Verify
(optional:, signed certificate sent to verify clients certificate)
Client Exchange
Change CipherSpec
(Signals transition in ciphering methods)
Finished
Change CIpherSpec
Finished
Cipher Change

Hello交换

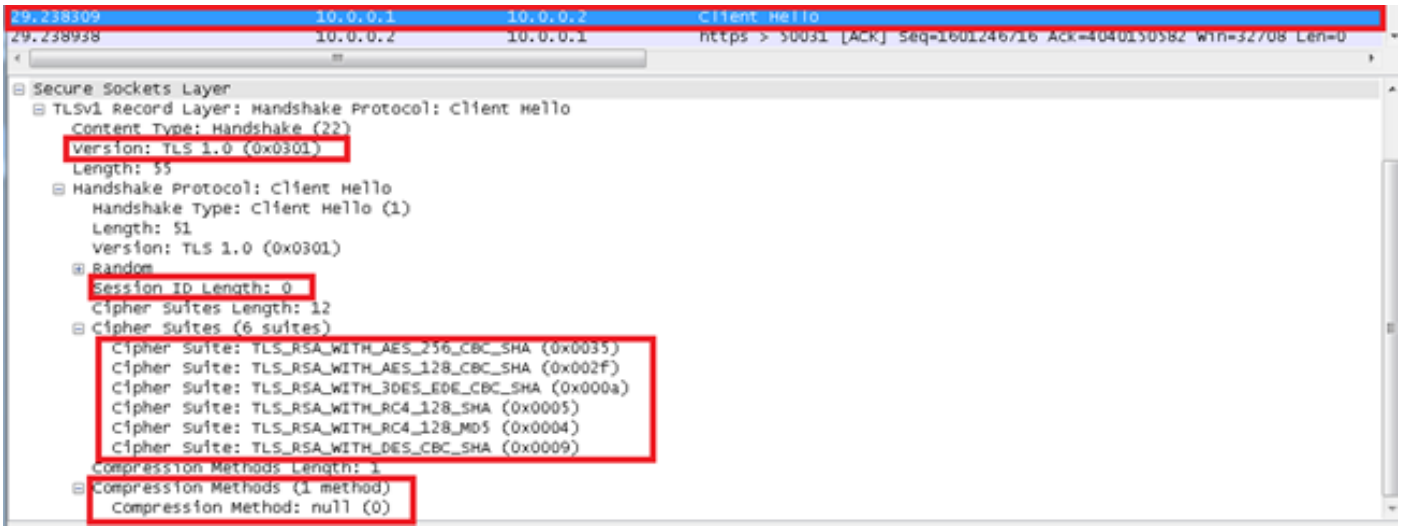
当SSL客户端和服务器开始通信时，它们会就协议版本达成一致，选择加密算法，或者相互验证，并使用公钥加密技术来生成共享密钥。这些进程在握手协议中执行。总之，客户端向服务器发送客户端Hello消息，服务器必须响应服务器Hello消息，否则会发生致命错误，并且连接失败。客户端Hello和服务器Hello用于在客户端和服务器之间建立安全增强功能。

客户端问候消息

客户端Hello将以下属性发送到服务器：

- **协议版本:**客户端在此会话期间希望通信的SSL协议版本。
- **会话 ID:**客户端希望用于此连接的会话的ID。在交换的第一个客户端Hello中，会话ID为空（请参阅注释后的数据包捕获屏幕截图）。
- **密码套件：**这会在客户端Hello消息中从客户端传递到服务器。它包含按客户端偏好顺序（首选）由客户端支持的加密算法组合。 每个密码套件定义密钥交换算法和密码规范。服务器选择密码套件，或者，如果未提供可接受的选择，则返回握手失败警报并关闭连接。
- **压缩方法:**包括客户端支持的压缩算法列表。如果服务器不支持客户端发送的任何方法，连接将失败。压缩方法也可以为null。

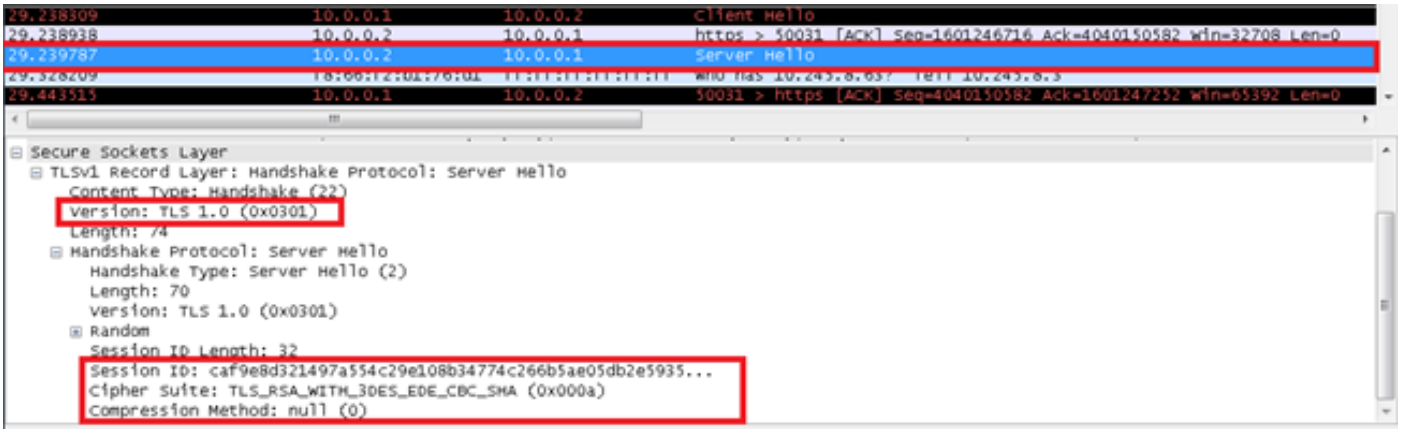
注意：捕获中的服务器IP地址为10.0.0.2，客户端IP地址为10.0.0.1。



服务器问候消息

服务器将以下属性发回客户端：

- **协议版本:**客户端支持的SSL协议的选定版本。
- **会话 ID:**这是与此连接对应的会话的标识。如果客户端在客户端Hello中发送的会话ID不为空，则服务器在会话缓存中查找匹配项。如果找到匹配项，并且服务器愿意使用指定的会话状态建立新连接，则服务器会以客户端提供的相同值作出响应。这表示会话已恢复，并指示各方必须直接继续处理已完成的消息。否则，此字段包含标识新会话的不同值。服务器可能会返回空 **session_id** ，以指示会话不会缓存，因此无法恢复。
- **密码套件：**由服务器从客户端发送的列表中选择。
- **压缩方法:**由服务器从客户端发送的列表中选择。
- **证书请求:**服务器向客户端发送其上配置的所有证书的列表，并允许客户端选择要用于身份验证的证书。

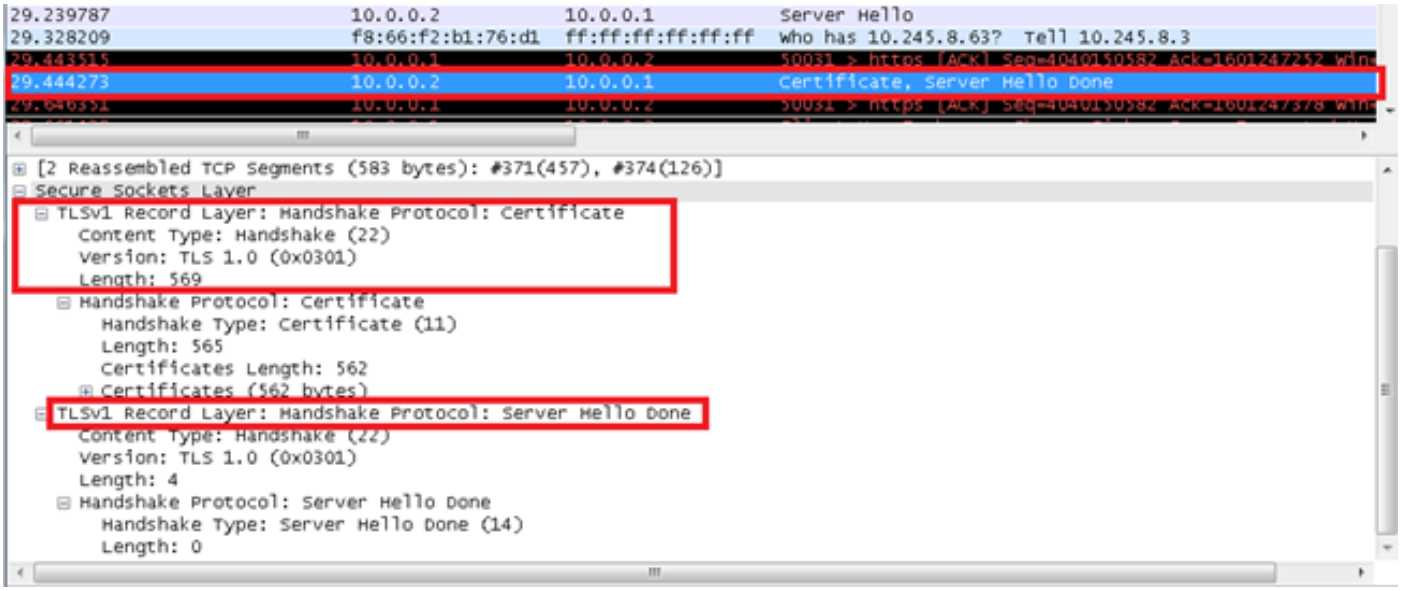


对于SSL会话恢复请求：

- 服务器也可以向客户端发送Hello请求。这只是为了提醒客户端，它应在方便时使用客户端Hello请求开始重新协商。如果握手过程已在进行中，客户端会忽略来自服务器的Hello请求。
- 握手消息比传输应用数据更优先。重新协商必须在不超过最大长度应用数据消息传输时间的1到2倍内开始。

服务器Hello完成

服务器发送Hello Done消息，以指示服务器hello消息和关联消息的结束。发送此消息后，服务器会等待客户端响应。在收到Server Hello Done消息后，客户端会验证服务器是否提供了有效的证书（如果需要），并检查服务器Hello参数是否可接受。



服务器证书、服务器密钥交换和证书请求（可选）

- **服务器证书**：如果服务器必须经过身份验证（通常情况下），则服务器会在服务器Hello消息后立即发送其证书。证书类型必须适用于所选密码套件密钥交换算法，且通常为X.509.v3证书。
- **服务器密钥交**换：如果服务器没有证书，则服务器会发送服务器密钥交换消息。如果服务器证书中包含Diffie-Hellman(DH)参数，则不使用此消息。
- **证书请求**：服务器可以根据所选密码套件的需要从客户端请求证书。

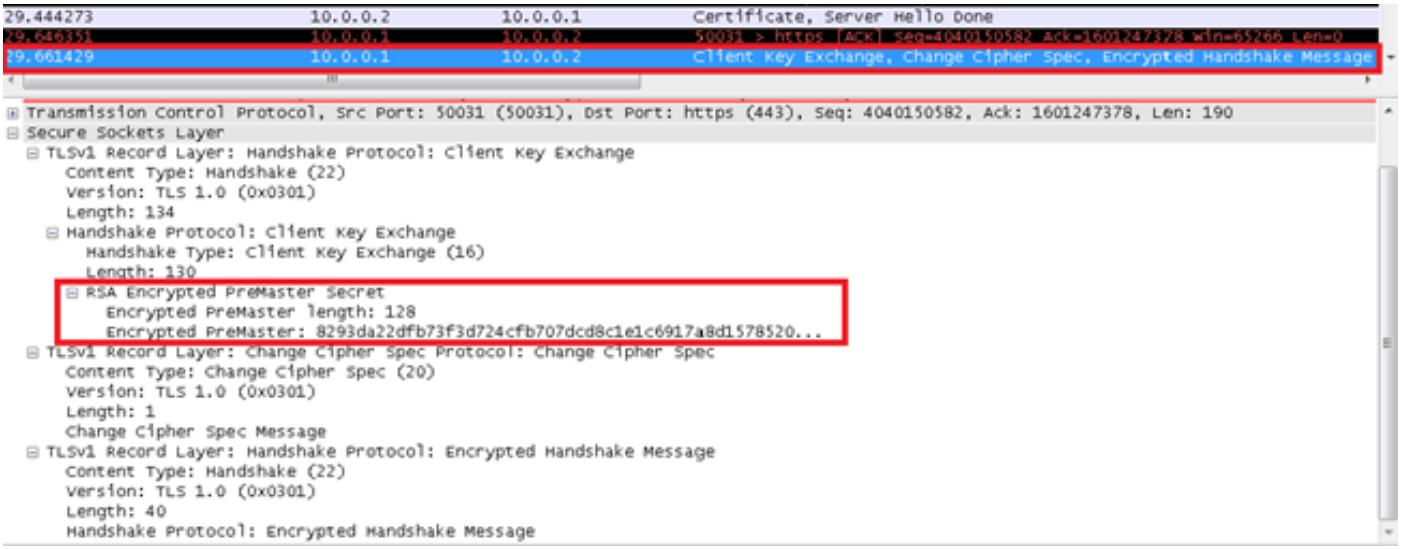
客户端交换

客户端证书（可选）

这是客户端在收到服务器Hello Done消息后发送的第一条消息。此消息仅在服务器请求证书时发送。如果没有合适的证书可用，则客户端会发送no_certificate警报。此警报仅是警告；但是，如果需要客户端身份验证，服务器可能会发出致命握手失败警报。客户端DH证书必须与服务器指定的DH参数匹配。

客户端密钥交换

此消息的内容取决于在客户端Hello消息和服务器Hello消息之间选择的公钥算法。客户端使用由Rivest-Shamir-Addleman(RSA)算法加密的预主密钥或DH进行密钥协议和身份验证。当RSA用于服务器身份验证和密钥交换时，客户端将生成一个48字节的pre_master_secret，在服务器公钥下加密，然后发送到服务器。服务器使用私钥来解密pre_master_secret。然后，双方将pre_master_secret转换为master_secret。



证书验证（可选）

如果客户端发送具有签名功能的证书，则会发送数字签名的证书验证消息以明确验证证书。

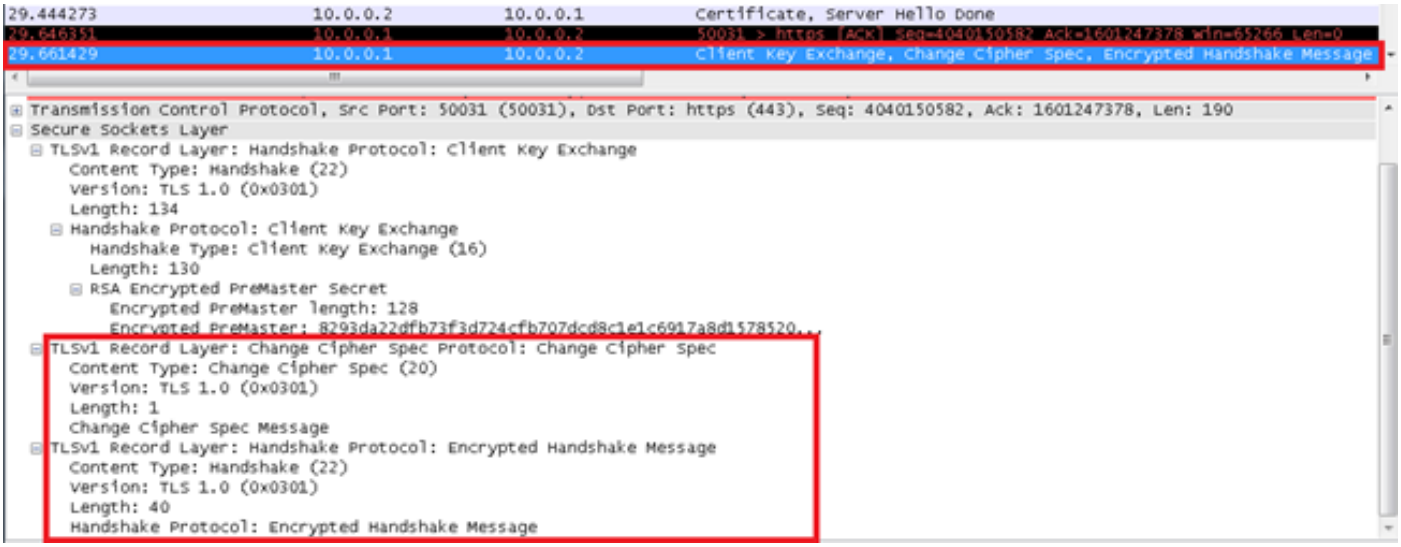
密码更改

更改密码规范消息

更改密码规范消息由客户端发送，客户端将待处理的密码规范（新密码规范）复制到当前密码规范（以前使用的密码规范）中。 变更密码规范协议是为了在加密策略中发出转换信号而存在的。该协议由单条消息组成，在当前（非待处理的）密码规范下加密和压缩。该消息由客户端和服务器发送，以通知接收方，后续记录受最近协商的密码规范和密钥保护。接收此消息导致接收方将读取挂起状态复制到读取当前状态。客户端在握手密钥交换和证书验证消息（如果有）后发送更改密码规范消息，服务器在成功处理从客户端收到的密钥交换消息后发送一条消息。恢复上一会话后，Change Cipher Spec消息在Hello消息后发送。在捕获中，客户端交换、更改密码和完成消息作为来自客户端的单条消息发送。

已完成邮件

始终在更改密码规范消息后立即发送完成消息，以验证密钥交换和身份验证过程是否成功。“完成”消息是第一个使用最近协商的算法、密钥和机密的受保护数据包。无需确认“完成”消息；当各方发送完成消息后，可以立即开始发送加密数据。已完成邮件的收件人必须验证内容是否正确。



相关信息

- [RFC 6101 — 安全套接字层协议版本3.0]
- [Wireshark SSL Wiki] — 使用Wireshark解密SSL数据包
- [技术支持和文档 - Cisco Systems]