SSL Inleiding met Sample Transaction and Packet Exchange

Inhoud

Inleiding

Dit document beschrijft de basisconcepten van het SSL-protocol (Secure Socket Layer) en biedt een steekproeftransactie en een pakketvastlegging.

Overzicht van SSL-record

De basiseenheid van gegevens in SSL is een record. Elk record bestaat uit een header van vijf bytes, gevolgd door gegevens.

Formaat opnemen

- Type: uint8 - genoteerde waarden
- **Versie**: uint16
- **Length:** uint16

Type	Versie		Lengte	
O	VH	VL	LH	LL

Type opname

Er zijn vier record-types in SSL:

- **Handdruk** (22, 0x16)
- **Spreek van schrijfmachine wijzigen** (20, 0x14)
- **Waarschuwing** (21, 0x15)
- **Toepassingsgegevens** (23, 0x17)

Record versie

De platforversie is een waarde van 16 bits en is in netwerkvolgorde geformatteerd.

> Opmerking: Voor SSL versie 3 (SSLv3) is de versie 0x0300. Voor Transport Layer Security versie 1 (TLSv1) is de versie 0x0301. De Cisco adaptieve security applicatie (ASA) ondersteunt SSL versie 2 (SSLv2), die versie 0x002 of een versie van TLS groter dan TLS gebruikt v1.

Lengte opnemen

De recordlengte is een waarde van 16 bytes en wordt in netwerkvolgorde geformatteerd.

In theorie betekent dit dat één record kan oplopen tot 65.535 (2^16-1) bytes. TLSv1 RFC2246 stelt dat de maximale lengte 16.383 (2^14-1) bytes is. Het is bekend dat Microsoft-producten (Microsoft Internet Explorer en Internet Information Services) deze grenzen overschrijden.

Soorten dossiers

In deze sectie worden de vier typen SSL-records beschreven.

Handshake records

De dossiers van de handdruk bevatten een reeks berichten die worden gebruikt om handdruk te maken. Dit zijn de boodschappen en hun waarden:

- **Hallo aanvraag** (0, 0x00)
- **ClientHallo** (1, 0x01)
- **Server Hallo** (2, 0x02)
- **Certificaat** (11, 0x0B)
- **Server Key exchange** (12, 0x0C)
- **certificaataanvraag** (13, 0x0D)
- **Server Hallo gedaan** (14, 0x0E)
- **Verificatie** (15, 0x0F)
- **Clientuitwisseling** (16, 0x10)
- **Klaar** (20, 0x14)

In het simpele geval, worden de handdruk records niet versleuteld. Een handdruk-record die een afgewerkt bericht bevat wordt echter altijd versleuteld, omdat dit altijd voorkomt na een Change Cipher Spec (CCS)-record.

CCS-records

CCS records worden gebruikt om een verandering in cryptografische cifers aan te geven. Direct na het opnemen van de CCS worden alle gegevens versleuteld met het nieuwe algoritme. CCS-bestanden kunnen al dan niet worden versleuteld; in een eenvoudige verbinding met één handdruk wordt het CCS - record niet versleuteld .

Waarschuwingsgegevens

Alarmgegevens worden gebruikt om de peer aan te geven dat een aandoening heeft plaatsgevonden. Sommige waarschuwingen zijn waarschuwingen, terwijl andere fataal zijn en de verbinding verbroken is. Waarschuwingen kunnen al dan niet versleuteld worden en kunnen voorkomen tijdens een handdruk of tijdens de gegevensoverdracht. Er zijn twee soorten signaleringen:

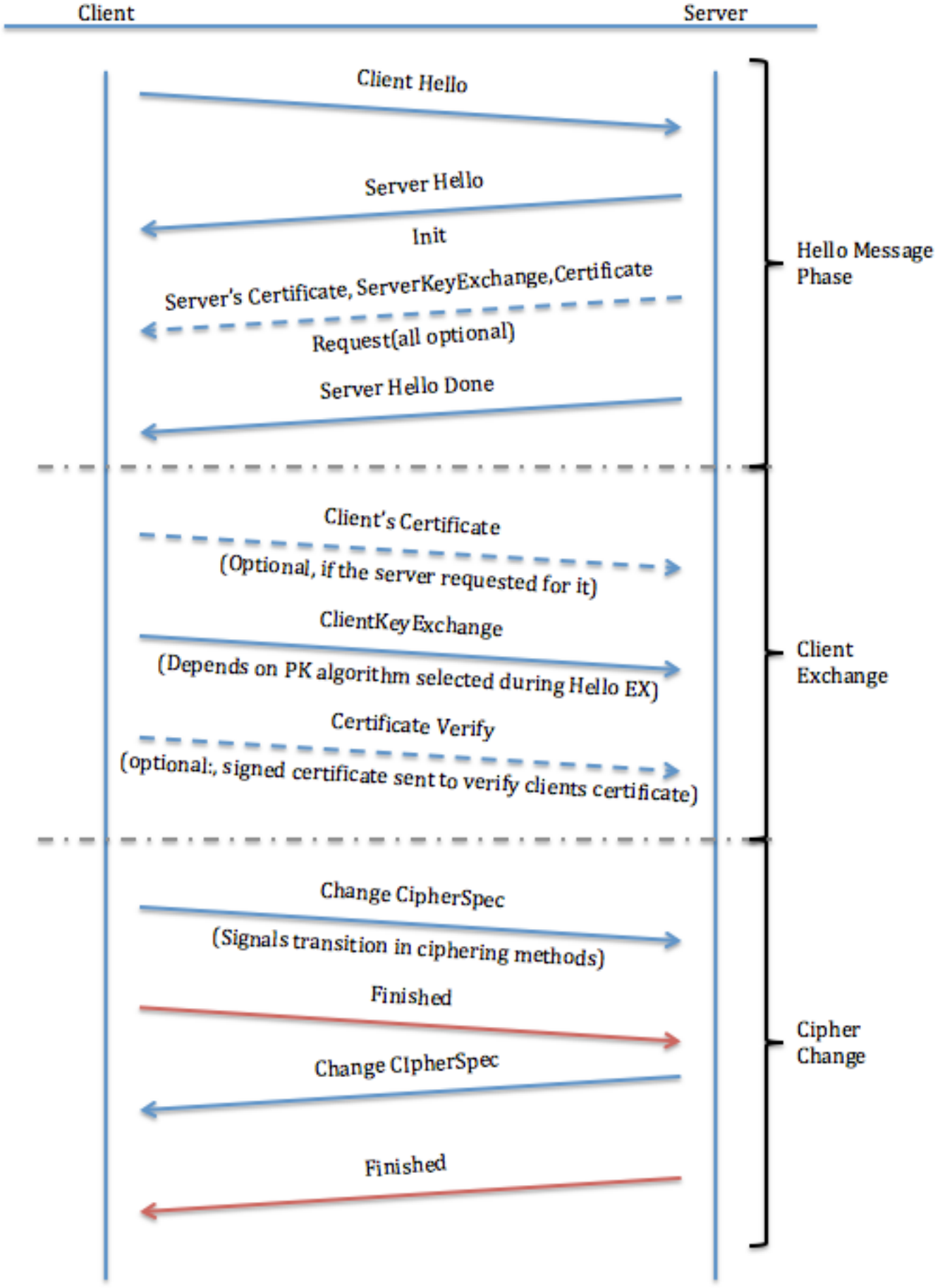
- **Waarschuwingen sluiten:** De verbinding tussen de client en de server moet goed gesloten zijn om storingen te voorkomen. Een **close_notification** wordt verstuurd dat aan de ontvanger aangeeft dat de afzender geen berichten meer zal verzenden op die verbinding.
- **Fout in meldingen:** Wanneer een fout wordt gedetecteerd, stuurt de detecterende partij een bericht naar de andere partij. Na verzending of ontvangst van een fataal waarschuwingsbericht sluiten beide partijen onmiddellijk de verbinding. Een aantal voorbeelden van foutmeldingen zijn:
  - **onverwacht_bericht** (fataal)
  - **decompressie_falen**
  - **handdruk_storing**

Toepassingsgegevensrecord

Deze registers bevatten de eigenlijke toepassingsgegevens. Deze berichten worden gedragen door de opnamelaag en gefragmenteerd, gecomprimeerd en versleuteld, op basis van de huidige verbindingsstaat.

Monstertransactie

In deze sectie wordt een steekproeftransactie tussen de client en de server beschreven.



De Hallo Exchange

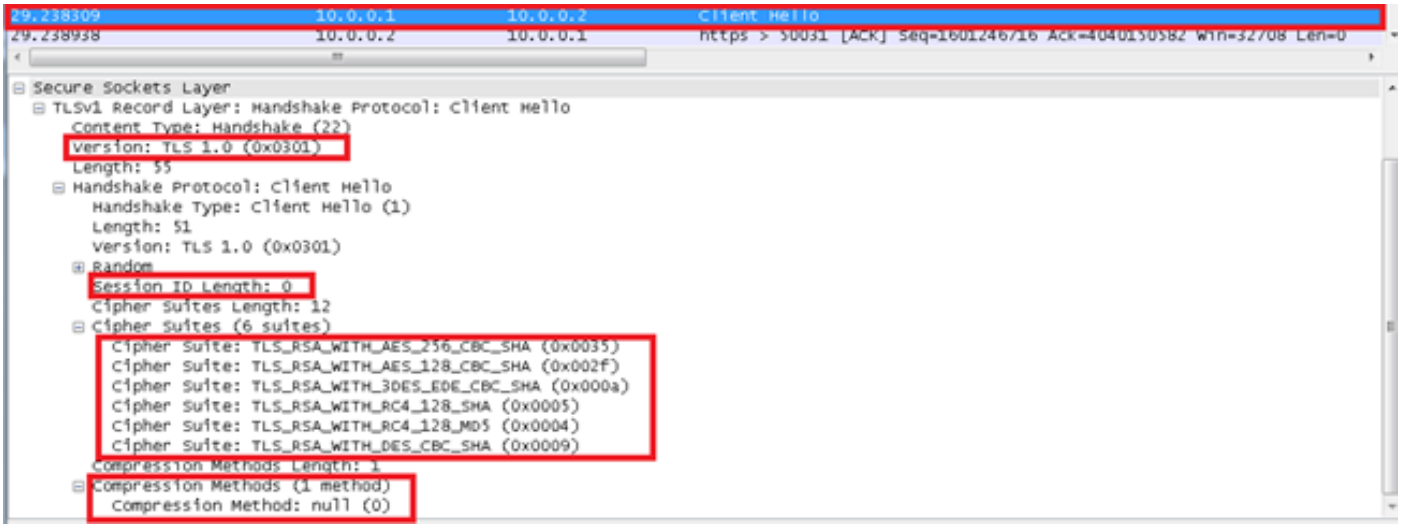
Wanneer een SSL client en server beginnen te communiceren, gaan ze akkoord met een protocolversie, selecteert u cryptografische algoritmen, selecteert u elkaar optioneel en gebruikt u openbare sleutelencryptietechnieken om gedeelde geheimen te genereren. Deze processen worden uitgevoerd in het handdruk-protocol. Samengevat, verstuurt de client een bericht van de klant naar de server, die moet reageren met een bericht van de server of een fatale fout optreedt en de verbinding faalt. De ClientHallo en de Server Hallo worden gebruikt om de beveiligingsfuncties tussen de client en de server in te stellen.

ClientHallo

De client geeft deze eigenschappen naar de server door:

- **Protocolversie:** De versie van het SSL-protocol waarmee de client tijdens deze sessie wil communiceren.
- **Session-id:** De ID van een sessie die de cliënt voor deze verbinding wenst te gebruiken. In de eerste Client Hallo van de uitwisseling, is de sessie-ID leeg (raadpleeg de pakketopnamescherm die na de opmerking wordt opgenomen).
- **Gebruikershandleiding:** Dit wordt van de client naar de server in het bericht van de Clientgroep doorgegeven. Het bevat de combinaties van cryptografische algoritmen die door de cliënt worden ondersteund in volgorde van voorkeur van de cliënt (eerste keuze). Elke algoritme definieert zowel een algoritme voor een belangrijke uitwisseling als een algoritme. De server selecteert een algoritmische reeks of, als er geen acceptabele keuzes worden voorgesteld, geeft hij een fout terug en sluit de verbinding.
- **Compressiemethode:** Omvat een lijst met compressiemethoden die door de client worden ondersteund. Als de server geen methode ondersteunt die door de client wordt verstuurd, mislukt de verbinding. De compressiemethode kan ook ongeldig zijn.

Opmerking: Het IP-adres van de server is 10.0.0.2 en het IP-adres van de client is 10.0.0.1.



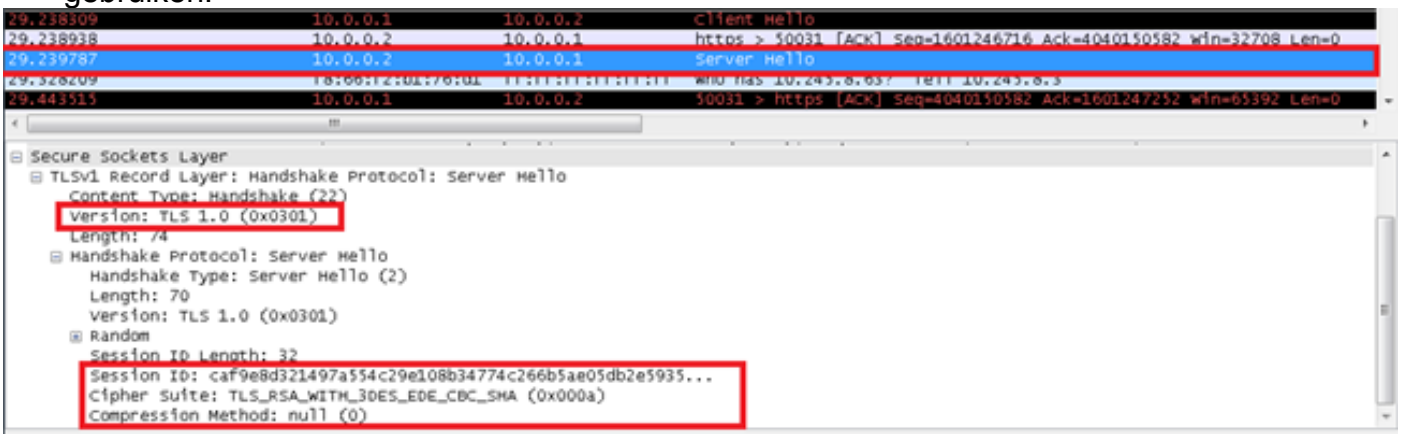
ServerHallo

De server stuurt deze eigenschappen terug naar de client:

- **Protocolversie:** De gekozen versie van het SSL-protocol dat de client ondersteunt.
- **Session-id:** Dit is de identiteit van de sessie die overeenkomt met dit verband. Als de sessie-ID die door de client in de client wordt verstuurd niet leeg is, ziet de server in de sessie cache

voor een match. Als een match gevonden wordt en de server bereid is om de nieuwe verbinding op te zetten met de gespecificeerde sessiestatus, reageert de server met dezelfde waarde die door de client geleverd werd. Dit duidt op een hervatting van de vergadering en dicteert dat de partijen rechtstreeks naar de eindberichten moeten gaan. Anders bevat dit veld een andere waarde die de nieuwe sessie identificeert. De server kan een lege **sessie_id** teruggeven om aan te geven dat de sessie niet gecached zal worden en kan daarom niet hervat worden.

- **Gebruikershandleiding:** Zoals geselecteerd door de server uit de lijst die van de cliënt werd verzonden.
- **Compressiemethode:** Zoals geselecteerd door de server uit de lijst die van de cliënt werd verzonden.
- **certificaataanvraag:** De server stuurt de client een lijst met alle certificaten die er op zijn ingesteld en stelt de client in staat om te selecteren welk certificaat ze voor verificatie wil gebruiken.

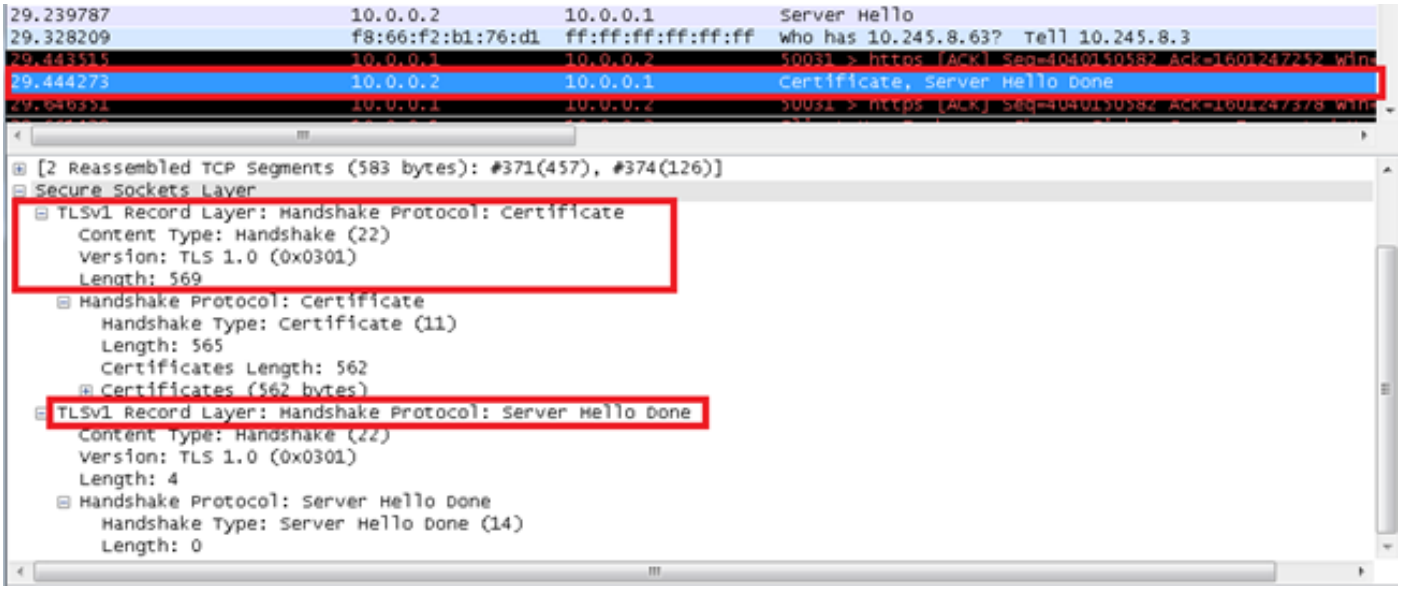


Voor SSL sessieverzoeken:

- De server kan ook een verzoek van Hallo naar de cliënt sturen. Dit is alleen om de klant eraan te herinneren dat hij de heronderhandeling moet starten met een verzoek van Client Hallo wanneer dat handig is. De client negeert het Hallo verzoek van de server als het handshake-proces al aan de gang is.
- De handdruk berichten hebben meer voorrang op de transmissie van toepassingsgegevens. De heronderhandeling moet beginnen binnen één of twee keer de zendtijd van een maximale lengte van een toepassingsgegevensbericht.

Gereed voor server

Het bericht Gereedschap van de server wordt door de server verzonden om het einde van de server en bijbehorende berichten aan te geven. Nadat het dit bericht verstuurt, wacht de server op een client antwoord. Na ontvangst van het bericht "Hallo server" verifieert de client dat de server indien nodig een geldig certificaat had verstrekt en controleert of de parameters van de server Hallo aanvaardbaar zijn.



Server certificaataanvraag, vervanging van server en certificaataanvraag (optioneel)

- **servercertificaat:** Als de server beveiligd moet zijn (wat in het algemeen het geval is), stuurt de server het certificaat direct na het bericht "Hallo server". Het certificaat type moet geschikt zijn voor het geselecteerde algoritme voor de uitwisseling van algoritme en is in het algemeen een X.509.v3 certificaat.
- **Server Key Exchange:** Het Server Key Exchange-bericht wordt door de server verstuurd als het geen certificaat heeft. Als de parameters Diffie-Hellman (DH) bij het servercertificaat zijn inbegrepen, wordt dit bericht niet gebruikt.
- **certificaataanvraag:** Een server kan optioneel een certificaat van de client aanvragen, indien van toepassing voor de geselecteerde doelreeks.

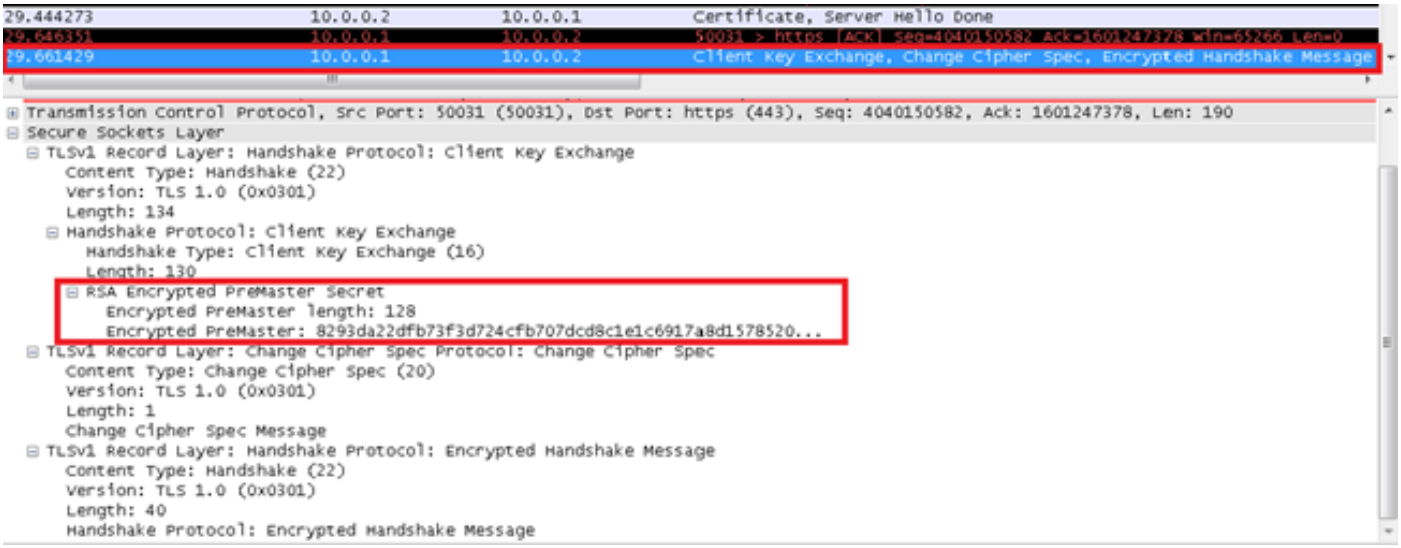
Clientexchange

Clientcertificaat (optioneel)

Dit is het eerste bericht dat de klant verstuurt nadat hij/zij een bericht van de Server Hallo ontvangt. Dit bericht wordt alleen verzonden als de server om een certificaat vraagt. Als er geen geschikt certificaat beschikbaar is, verstuurt de client juist een waarschuwing **no_certificaat**. Deze waarschuwing is slechts een waarschuwing; de server kan echter reageren met een fatale fout signalering als de client beveiligd is . De client-DH-certificaten moeten overeenkomen met de server-opgegeven DH-parameters.

Clientuitwisseling

De inhoud van dit bericht is afhankelijk van het openbare algoritme dat tussen de berichtjes van de Cliënt en de Server Hallo is geselecteerd. De client gebruikt ofwel een premaster-sleutel versleuteld met het Rivest-Shamir-Addleman (RSA)-algoritme of DH voor een belangrijke overeenkomst en verificatie. Wanneer RSA gebruikt wordt voor server authenticatie en key exchange, wordt een 48-byte **pre_master_geheven** door de client, gecodeerd onder de server public key, en verzonden naar de server. De server gebruikt de privé sleutel om de **pre_master_geheven** te decrypteren. Beide partijen converteren vervolgens de **pre_master_SECURITY** naar de **master_SECURITY**.



Certificaat controleren (optioneel)

Als de klant een certificaat verstuurt met de ondertekeningsmogelijkheid, wordt een digitaal ondertekend certificaatverificatiebericht verstuurd om het certificaat expliciet te controleren.

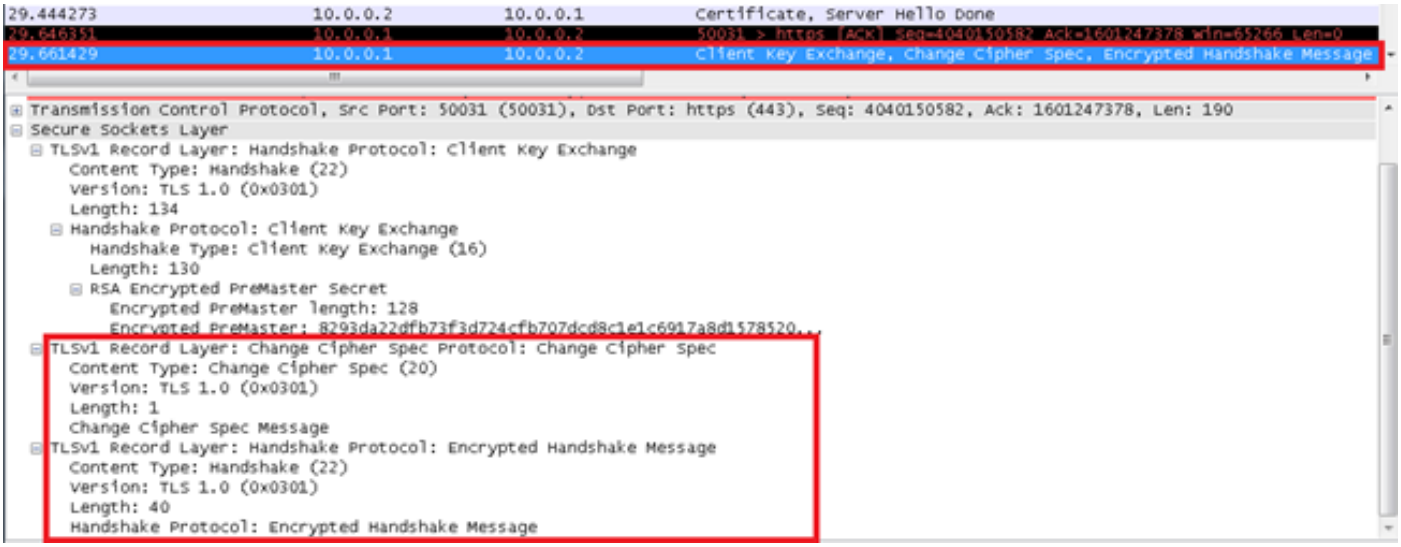
Cipher Change

Spec-berichten van gebruiker wijzigen

Het speciale bericht van het wisselkantoor wordt door de client verstuurd en de client kopieert de hangende cipher Spec (de nieuwe) naar de huidige cipher Spec (de eerder gebruikte). Het protocol van Cipher Spec bestaat om overgangen in algoritmische strategieën te signaleren. Het protocol bestaat uit één bericht, dat versleuteld en gecomprimeerd is onder de huidige (niet de hangende) samenvatting van het algoritme. Het bericht wordt verzonden door zowel de client als de server om de ontvangende partij ervan in kennis te stellen dat opeenvolgende records beschermd zijn onder de meest recent overeengekomen sleutels van de klant en sleutels. Het ontvangen van dit bericht veroorzaakt dat de ontvanger de gelezen hangende staat in de gelezen huidige staat kopieert. De client verstuurt een voicemailbericht nadat de handdruk-toets is uitgewisseld en de certificaatcontrole-berichten (indien aanwezig) zijn verstuurd en de server verstuurt een bericht nadat de belangrijke uitwisselingsbericht dat de client heeft ontvangen, met succes is verwerkt. Wanneer een vorige sessie wordt hervat, wordt het bericht Spraak van het wisselaar verstuurd na de Hallo berichten. In de opnames, worden de de Uitwisseling van de Cliënt, het vergissing, en de Klaar berichten verzonden als één bericht van de cliënt.

Eindberichten

Een voltooid bericht wordt altijd onmiddellijk na een speciaal bericht van het Change-algoritme verstuurd om na te gaan of de belangrijkste uitwisselings- en verificatieprocessen succesvol waren. Het eindigende bericht is het eerste beschermde pakket met de meest recent overeengekomen algoritmen, sleutels en geheimen. Er is geen ontvangstbevestiging van het eindigende bericht vereist. De partijen kunnen beginnen gecodeerde gegevens onmiddellijk te verzenden nadat zij het EINDbericht hebben verzonden. Ontvangers van de eindigende berichten moeten nagaan of de inhoud juist is.



Gerelateerde informatie

- RFC 6101 - The Secure Socrates Layer Protocol, versie 3.0
- Wireshark SSL wiki - decrypteer SSL-pakketten met Wireshark
- Technische ondersteuning en documentatie – Cisco Systems