مقدمة SSL مع نموذج الحركة وتبادل الحزم

المحتويات

المقدمة

يصف هذا المستند المفاهيم الأساسية لبروتوكول طبقة مآخذ التوصيل الآمنة (SSL)، ويقدم نموذجا للمعاملات ومميزة التقاط الحزم.

نظرة عامة على سجل SSL

الوحدة الأساسية للبيانات في SSL هي سجل. يتكون كل سجل من رأس سجل مكون من خمسة بايت، متبوعا بالبيانات.

تنسيق السجل

- **النوع**: uINT8 - القيمة المسرودة
- **الإصدار**: uINT16
- **الطول**: uINT16

النوع	الإصدار		طول	
ت	VH	VL	LH	LL

نوع السجل

هناك أربعة أنواع من السجلات في SSL:

- **مصافحة** (22، 0x16)
- **تغيير مواصفات التشفير** (20، 0x14)

- **تنبيه** (21، 0x15)
- **بيانات التطبيق** (23، 0x17)

إصدار السجل

إصدار السجل عبارة عن قيمة 16 بت وتم تنسيقه بترتيب الشبكة.

> **ملاحظة**: بالنسبة لإصدار 3 من SSL (SSLv3)، يكون الإصدار 0x0300. بالنسبة لإصدار أمان طبقة النقل 1 (TLSv1)، يكون الإصدار 0x0301. لا يدعم جهاز الأمان القابل للتكيف (ASA) من Cisco الإصدار 2 من SSL (SSLv2)، الذي يستخدم الإصدار 0x0002، أو أي إصدار من TLS أكبر من TLSv1.

طول السجل

طول السجل هو قيمة 16 بايت وتم تنسيقه بترتيب الشبكة.

من الناحية النظرية، هذا يعني أن السجل الواحد يمكن أن يصل طوله إلى 65،535 (2^16 -1) بايت. يشير TLSv1 RFC2246 إلى أن الحد الأقصى للطول هو 16383 (2^14 -1) بايت. من المعروف أن منتجات Microsoft (Microsoft Internet Explorer و Internet Information Services) تتجاوز هذه الحدود.

أنواع السجلات

يصف هذا القسم الأنواع الأربعة من سجلات SSL.

سجلات المصافحة

تحتوي سجلات المصافحة على مجموعة من الرسائل التي يتم إستخدامها من أجل المصافحة. هذه هي الرسائل وقيمها:

- **طلب مرحبا** (0، 0x00)
- **Client Hello (**1، 0x01)
- **Server Hello (**2، 0x02)
- **الشهادة** (11، 0x0b)
- **تبادل مفتاح الخادم** (12، 0x0c)
- **طلب الشهادة** (13، 0x0d)
- **تم تنفيذ مرحبا بالخادم** (14، 0x0e)
- **التحقق من الشهادة** (15، 0x0f)
- **تبادل مفتاح العميل** (16، 0x10)
- **منتهي** (20، 0x14)

في الحالة البسيطة، التي يتم تشفير سجلات المصافحة. ومع ذلك، يتم دائما تشفير سجل المصافحة الذي يحتوي على رسالة مكتملة، حيث إنه يحدث دائما بعد سجل "مواصفات تشفير التغيير" (CCS).

سجلات CCS

يتم إستخدام سجلات CCS للإشارة إلى تغيير في تشفير التشفير. بعد تسجيل CCS

مباشرة، يتم تشفير جميع البيانات باستخدام التشفير الجديد. قد يتم تشفير سجلات CCS أو ال يتم تشفيرها؛ في اتصال بسيط بمصافحة واحدة، ال يتم تشفير سجل CCS.

سجلات التنبيه

يتم إستخدام سجلات التنبيه للإشارة إلى النظير إلى حدوث حالة. تعد بعض التنبيهات تحذيرات، في حين تكون التنبيهات الأخرى خطيرة وتتسبب في فشل الاتصال. قد يتم تشفير التنبيهات أو ال يتم، وقد تحدث أثناء مصافحة أو أثناء نقل البيانات. هناك نوعان من التنبيهات:

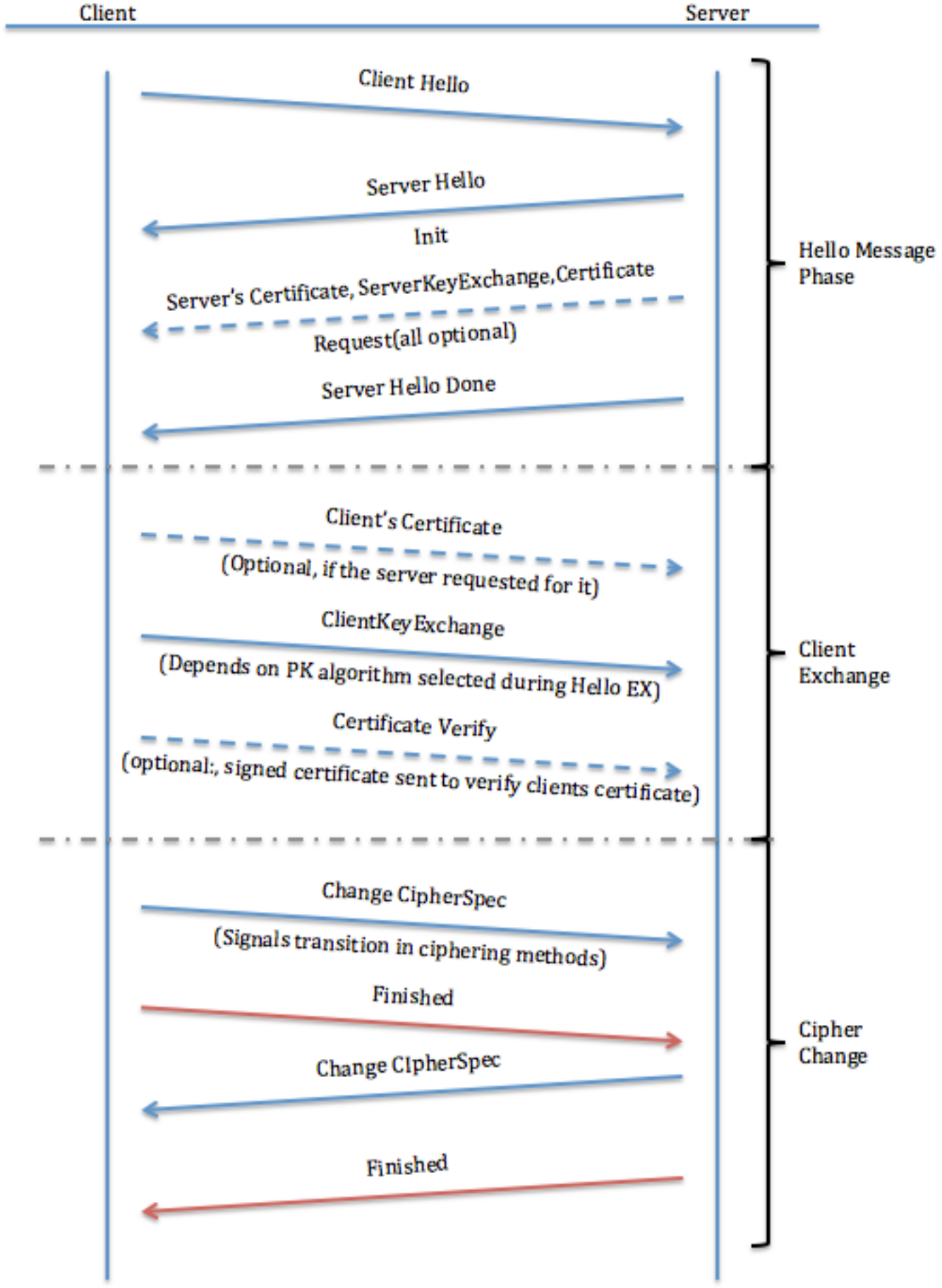
- **تنبيهات الإغلاق:** يجب إغلاق الاتصال بين العميل والخادم بشكل صحيح لتجنب أي نوع من هجمات الاقتطاع. يتم إرسال رسالة close_notify تشير إلى المستلم بأن المرسل لن يرسل رسائل بعد الآن على هذا الاتصال.
- **تنبيهات الخطأ:** عندما يتم الكشف عن خطأ، يرسل طرف الكشف رسالة إلى الطرف الآخر. عند إرسال رسالة تنبيه خطيرة أو تلقيها، يقوم كلا الطرفين بإغلاق الاتصال فورا. بعض الأمثلة على تنبيهات الأخطاء هي:
  - UNEXPECTED_MESSAGE (مميت)
  - إلغاء الضغط_الفشل
  - Handshake_failure

سجل بيانات التطبيق

تحتوي هذه السجلات على بيانات التطبيق الفعلية. يتم نقل هذه الرسائل بواسطة طبقة السجل ويتم تجزئتها وضغطها وتشفيرها، استنادا إلى حالة الاتصال الحالية.

نموذج الحركة

يصف هذا القسم عينة حركة بين العميل والخادم.


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

تبادل مرحبا

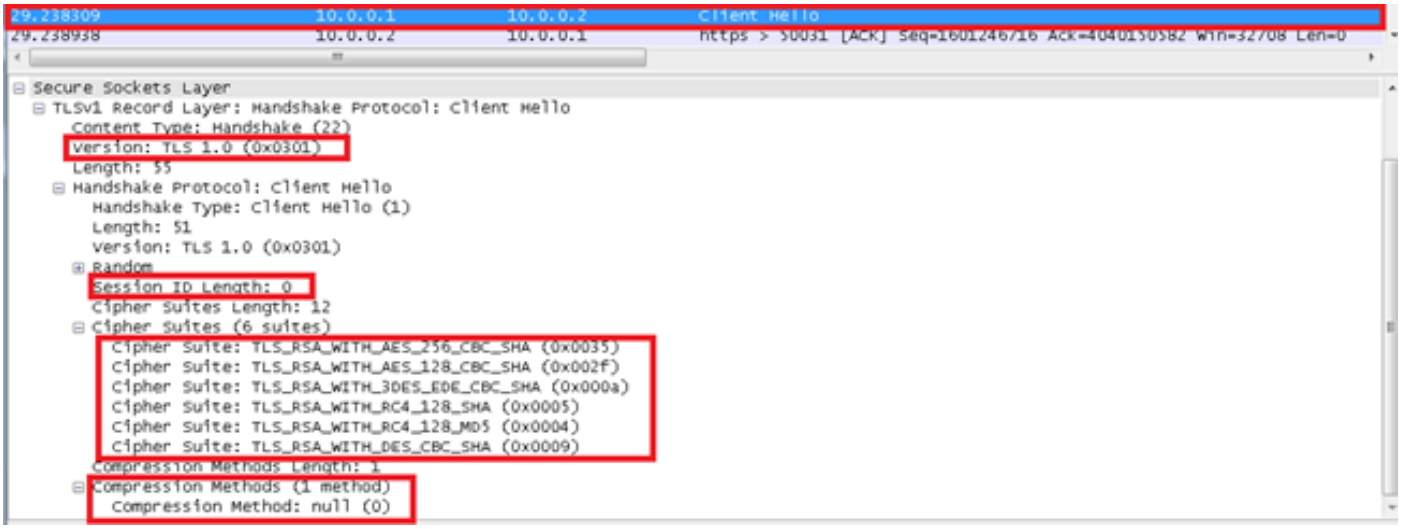
عند بدء اتصال عميل SSL والخادم، فإنهما يتفقان على إصدار بروتوكول وتحديد خوارزميات التشفير ومصادقة بعضهما البعض إختياريا واستخدام تقنيات تشفير المفتاح العام من أجل إنشاء أسرار مشتركة. يتم إجراء هذه العمليات في بروتوكول المصافحة. في الخلاصة، يرسل العميل رسالة Client Hello إلى الخادم، والتي يجب أن تستجيب برسالة Server Hello أو يحدث خطأ فادح وفشل الاتصال. يتم إستخدام Client Hello و Server Hello لإنشاء إمكانيات تحسين الأمان بين العميل والخادم.

Client Hello

يرسل Client Hello هذه السمات إلى الخادم:

- **إصدار البروتوكول:** إصدار بروتوكول SSL الذي يرغب العميل في الاتصال به أثناء جلسة العمل هذه.
- **معرف جلسة العمل:** معرف جلسة عمل يرغب العميل في إستخدامها لهذا الاتصال. في أول Client Hello من التبادل، يكون معرف الجلسة فارغا (راجع لقطة شاشة التقاط الحزمة بعد الملاحظة).
- **مجموعة تشفير:** يتم تمرير هذا من العميل إلى الخادم في رسالة Client Hello. وهو يحتوي على مجموعات من خوارزميات التشفير التي يدعمها العميل حسب تفضيله (الاختيار الأول). تقوم كل مجموعة تشفير بتعريف كل من خوارزمية تبادل المفاتيح وخوارزمية التشفير. يحدد الخادم مجموعة شفرة واحدة، في حالة عدم تقديم خيارات مقبولة، يرجع تنبيه فشل المصافحة ويغلق الاتصال.
- **أسلوب الضغط:** يتضمن قائمة لخوارزميات الضغط التي يدعمها العميل. إذا لم يعتمد الخادم أية طريقة يرسلها العميل، يفشل الاتصال. يمكن أن يكون أسلوب الضغط فارغا أيضا.

ملاحظة: عنوان IP للخادم في عمليات الالتقاط هو 10.0.0.2 وعنوان IP للعميل هو 10.0.0.1.



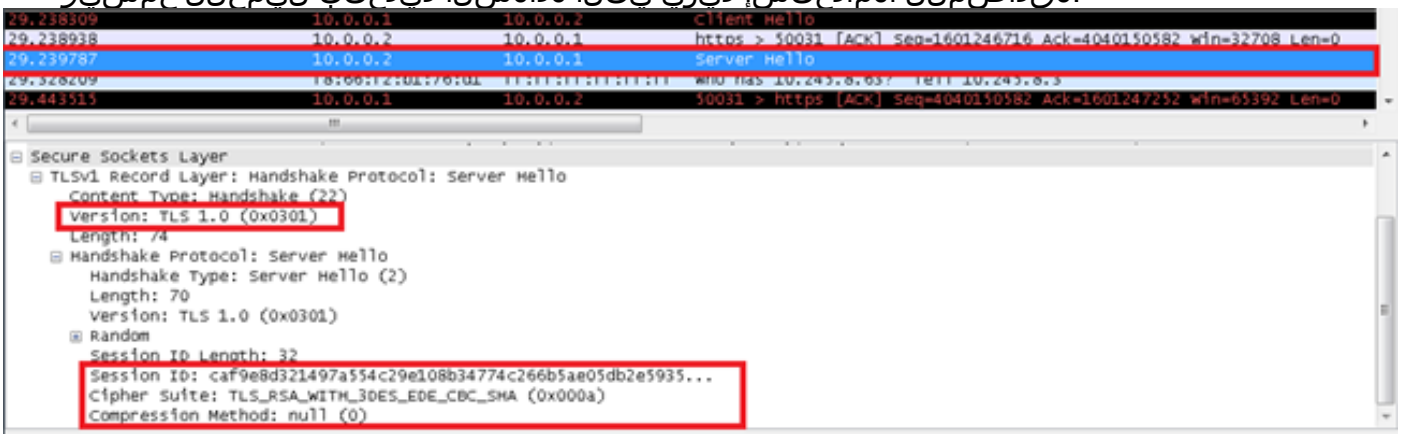
Server Hello

يرسل الخادم هذه السمات إلى العميل:

- **إصدار البروتوكول:** الإصدار المختار من بروتوكول SSL الذي يدعمه العميل.
- **معرف جلسة العمل:** هذا هو معرف جلسة العمل المطابقة لهذا الاتصال. إذا لم يكن معرف جلسة العمل الذي تم إرساله بواسطة العميل في Client Hello فارغا، يبحث الخادم في ذاكرة التخزين المؤقت لجلسة العمل بحثا عن تطابق. إذا تم العثور على تطابق وكان

الخادم على إستعداد لإنشاء اتصال جديد باستخدام حالة جلسة العمل المحددة، يستجيب الخادم بنفس القيمة التي تم توفيرها بواسطة العميل. وهذا يشير إلى انعقاد دورة مستأنفة ويفرض على الأطراف أن تنتقل مباشرة إلى الرسائل المنتهية. وإلا، يحتوي هذا الحقل على قيمة مختلفة تعرف الجلسة الجديدة. قد يقوم الخادم بإرجاع session_id فارغ للإشارة إلى عدم تخزين الجلسة مؤقتا، وبالتالي لا يمكن إستئنافها.

- **مجموعة التشفير:** كما هو محدد بواسطة الخادم من القائمة التي تم إرسالها من العميل.
- **أسلوب الضغط:** كما هو محدد بواسطة الخادم من القائمة التي تم إرسالها من العميل.
- **طلب الشهادة:** يرسل الخادم إلى العميل قائمة بجميع الشهادات التي تم تكوينها عليه، ويسمح للعميل بتحديد الشهادة التي يريد إستخدامها للمصادقة.

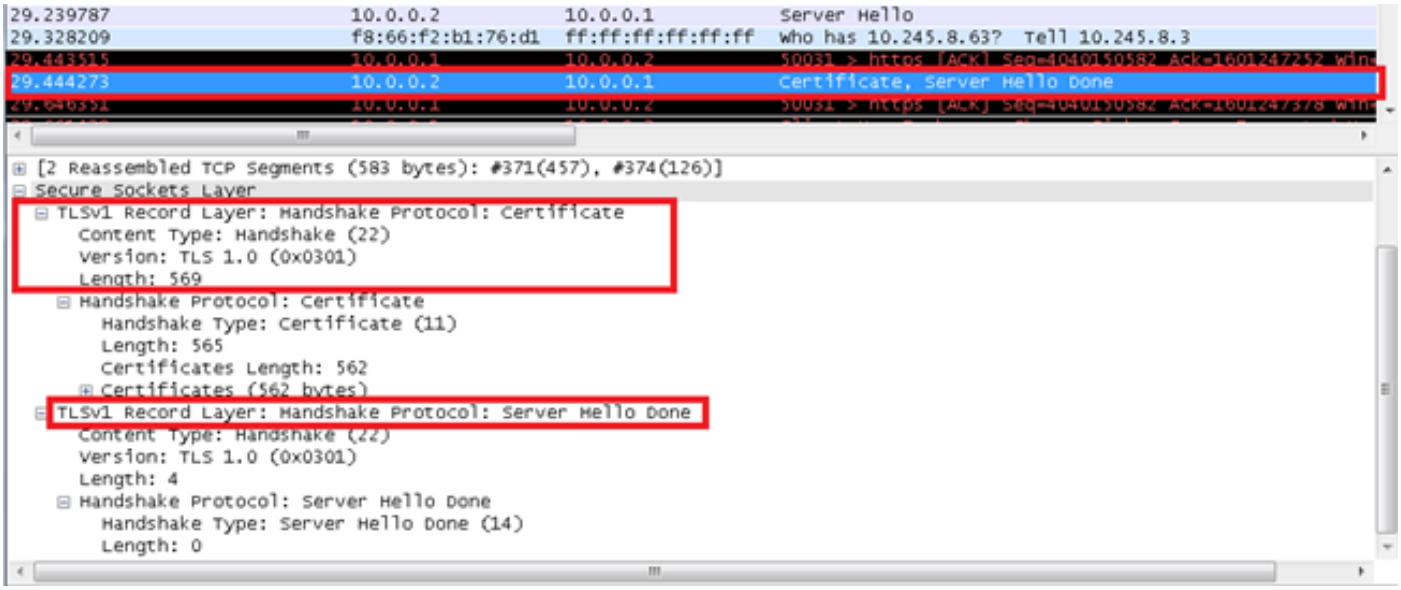


لطلبات إستئناف جلسة SSL:

- يمكن للخادم إرسال طلب "مرحبا" إلى العميل أيضا. وهذا فقط لتذكير العميل بأنه يجب عليه بدء إعادة التفاوض باستخدام طلب "مرحبا بالعميل" عندما يكون ذلك مناسبا. يتجاهل العميل طلب Hello من الخادم إذا كانت عملية مصافحة اليد قيد التنفيذ بالفعل.
- تكون لرسائل المصافحة أولوية أكبر على إرسال بيانات التطبيق. يجب أن تبدأ إعادة التفاوض مرة أو مرتين على الأكثر من وقت إرسال رسالة بيانات التطبيق ذات الطول الأقصى.

تم تنفيذ Server Hello

يتم إرسال رسالة "مرحبا بك في الخادم" بواسطة الخادم للإشارة إلى نهاية رسالة "مرحبا بك في الخادم" والرسائل المقترنة. بعد إرسال هذه الرسالة، ينتظر الخادم إستجابة العميل. عند إستلام رسالة Server Hello Done، يتحقق العميل من أن الخادم قدم شهادة صالحة، إذا كان ذلك مطلوبا، ويتحقق من أن معلمات Server Hello مقبولة.



شهادة الخادم، تبادل مفتاح الخادم، وطلب الشهادة (إختياري)

- **شهادة الخادم:** إذا كان يجب مصادقة الخادم (وهي الحالة بشكل عام)، يرسل الخادم شهادته مباشرة بعد رسالة Server Hello. يجب أن يكون نوع الشهادة مناسبا لخوارزمية تبادل مفاتيح مجموعة التشفير المحددة، وهو بشكل عام شهادة X.509.v3.
- **Server Key Exchange:** يتم إرسال رسالة Server Key Exchange بواسطة الخادم إذا لم يكن لديه شهادة. في حالة تضمين معلمات Diffie-Hellman (DH) مع شهادة الخادم، لا يتم إستخدام هذه الرسالة.
- **طلب الشهادة:** يمكن للخادم أن يطلب بشكل إختياري شهادة من العميل، إذا كان ذلك مناسبا لمجموعة التشفير المحددة.

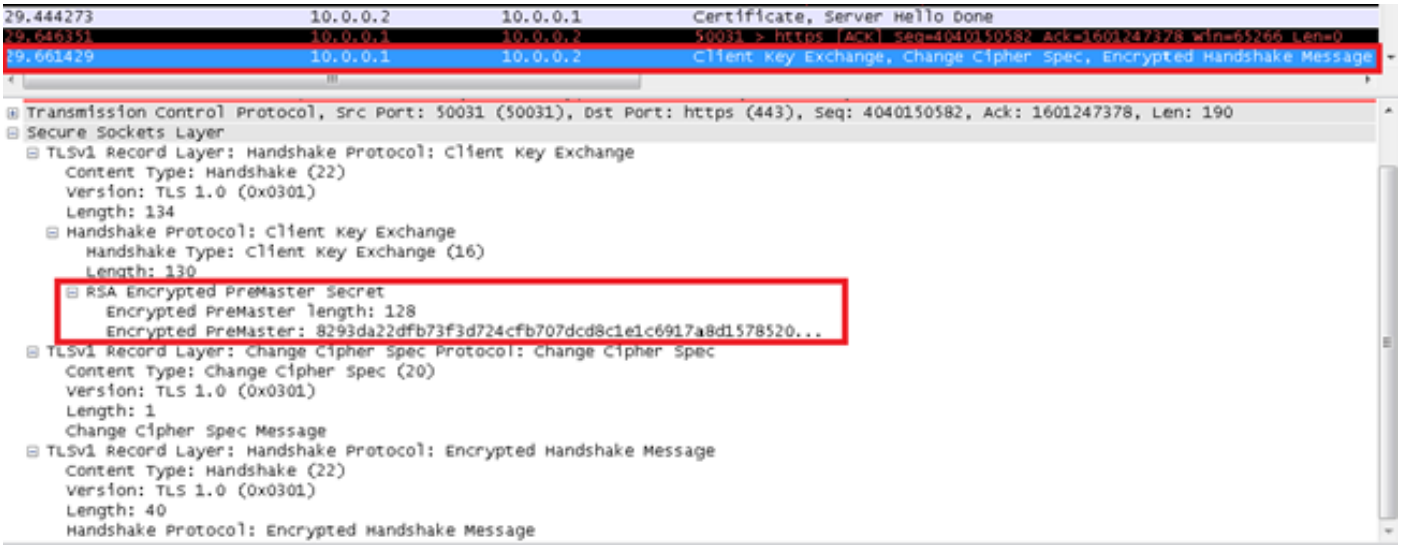
تبادل العملاء

شهادة العميل (إختيارية)

هذه هي الرسالة الأولى التي يرسلها العميل بعد أن يستلم رسالة "مرحبا بك في الخادم". يتم إرسال هذه الرسالة فقط إذا طلب الخادم شهادة. في حالة عدم توفر شهادة مناسبة، يرسل العميل تنبيه **no_certificate** بدلا من ذلك. هذا التنبيه هو تحذير فقط، ومع ذلك، قد يستجيب الخادم مع تنبيه فشل مصافحة هامة إذا كانت مصادقة العميل مطلوبة. يجب أن تتطابق شهادات DH الخاصة بالعميل مع معلمات DH المحددة للخادم.

تبادل مفتاح العميل

يعتمد محتوى هذه الرسالة على خوارزمية المفتاح العام المحددة بين رسائل Client Hello و Server Hello. يستخدم العميل إما مفتاح أساسي مشفر بواسطة خوارزمية Rivest-Shamir-Addleman (RSA) أو DH لاتفاقية المفتاح والمصادقة. عند إستخدام RSA لمصادقة الخادم وتبادل المفاتيح، يتم إنشاء **pre_master_secret** سعة 48 بايت بواسطة العميل، ويتم تشفيرها أسفل المفتاح العام للخادم، ويتم إرسالها إلى الخادم. يستخدم الخادم المفتاح الخاص لفك تشفير **pre_master_secret**. ثم يقوم كل الطرفين بتحويل **pre_master_secret** إلى **master_secret**.



التحقق من الشهادة (اختياري)

إذا أرسل العميل شهادة ذات إمكانية توقيع، يتم إرسال رسالة "التحقق من صحة الشهادة" موقعة رقميا للتحقق من الشهادة بشكل صريح.

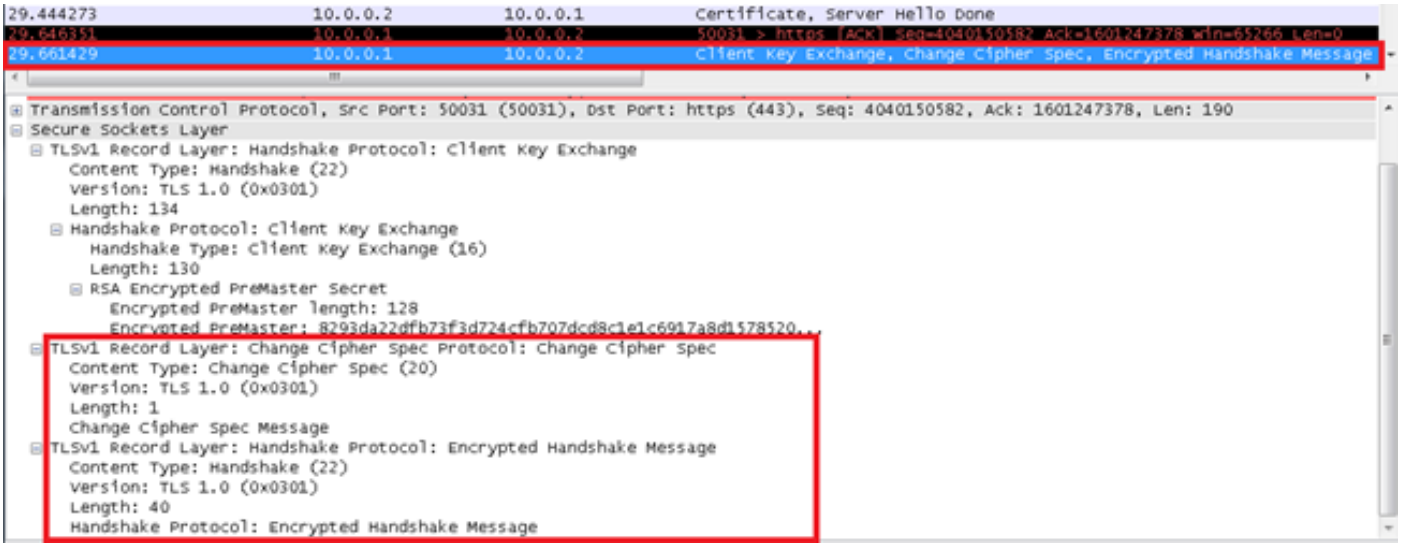
تغيير الشفرة

تغيير رسائل مواصفات التشفير

يتم إرسال رسالة "مواصفات تشفير التغيير" بواسطة العميل، ويقوم العميل بنسخ "مواصفات التشفير" المعلقة (الجديد) إلى "مواصفات التشفير" الحالية (تلك التي تم إستخدامها سابقا). يوجد بروتوكول مواصفات تشفير التغيير للإشارة إلى عمليات الانتقال في إستراتيجيات التشفير. يتكون البروتوكول من رسالة واحدة، يتم تشفيرها وضغطها بموجب مواصفات التشفير الحالية (غير المعلقة). يتم إرسال الرسالة بواسطة كل من العميل والخادم لإبلاغ الطرف المتلقي بأن السجلات التالية محمية بموجب أحدث مواصفات ومفاتيح التشفير التي تم التفاوض عليها. يؤدي إستلام هذه الرسالة إلى قيام المستلم بنسخ حالة القراءة المعلقة إلى الحالة الحالية المقروءة. يرسل العميل رسالة Change Cipher Spec بعد تبادل مفاتيح المصافحة ورسائل Certificate Verify (إن وجدت)، ويقوم الخادم بإرسال واحدة بعد أن يقوم بمعالجة رسالة تبادل المفاتيح التي تلقاها من العميل بنجاح. عند إستئناف جلسة عمل سابقة، يتم إرسال رسالة "تغيير مواصفات التشفير" بعد رسائل Hello. في عمليات الالتقاط، يتم إرسال رسائل Client Exchange و Change Cipher و End كرسالة واحدة من العميل.

الرسائل المنتهية

يتم دائما إرسال الرسالة "منتهية" مباشرة بعد رسالة "مواصفات تشفير التغيير" للتحقق من نجاح عمليتي تبادل المفاتيح والمصادقة. الرسالة المنتهي هي هي أول حزمة محمية مع أحدث الخوارزميات والمفاتيح والأسرار التي تم التفاوض عليها. الا يتطلب الأمر أي إقرار بالرسالة المنتهي؛ يمكن للأطراف البدء في إرسال بيانات مشفرة بعد إرسال الرسالة المنتهي مباشرة. يجب أن يتحقق مستلمو الرسائل المنتهية من صحة المحتويات.



معلومات ذات صلة

- [المعيار RFC 6101 - بروتوكول طبقة مآخذ التوصيل الآمنة الإصدار 3.0]
- [Wireshark SSL Wiki] - فك تشفير حزم SSL باستخدام Wireshark
- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).