UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad en Internet con los certificados SSL y HTTPS

Integrantes: **Gabriel Andrade**

Eric Borzone

Alonso Muñoz

Resumen

El protocolo HTTPS es un protocolo de comunicación segura, la cual puede utilizar certificados como el SSL, el cual tiene 3 tipos de certificados dependiendo de los requerimientos de la página web o dominio; en general los certificados buscan validad la autentificación y veracidad de un sitio web.

Introducción

Actualmente el ataque de agentes externos a las páginas web es un hecho común; por ende, tal como se requiere proteger los recintos privados con puertas y llaves, las páginas web deben tener seguridad en su autentificación al existir ataques como suplantación de la identidad, o espionaje de datos.

Definición de SSL

El certificado SSL es un protocolo de prueba de identidad de una página web. Cada página tiene su certificado propio (si lo desea), el cual es asignado por la *autoridad de certificación (CA)*. El CA se encarga de comprobar previamente la veracidad e identidad del sitio web.

Los certificados SSL son almacenados en el servidor, y son requeridos cada vez que un usuario visita una página web HTTPS.

Hay distintos tipos de certificación dependiendo del tipo de autentificación que ofrecen.

Tipos de certificado SSL

Certificados con validación de dominios (Domain Validated Certificate)

Es el tipo de certificado más rápido. La Autoridad de Certificación sólo corrobora si quien solicita el certificado es el propietario del dominio o no a certificar. Como no se comprueba ningún otro tipo de información, éste es el tipo de certificado más rápido y barato.

Éste tipo de certificado es adecuado para los sitios que no son propensos a riesgos de suplantación, fraude o phishing; además donde la credibilidad es secundario.

El phishing es un tipo de suplantación de identidad el cual se caracteriza por conseguir información confidencial de forma fraudulenta.

Certificados de validación de la organización o empresa (Organization Validated Certificate)

Este es un tipo de certificado más amplio y seguro que el de valoración de dominios, por ende es más caro. Además de verificar el propietario del dominio, se verifica información corporativa relevante; una vez corroborados estos datos, son observables por los usuarios, los cuales obtienen una mayor confianza del sitio web y la empresa.

Dicho certificado es adecuado para páginas donde se realicen transacciones que intercambias datos no sensibles.

Las páginas web que contengan Certificados SSL de organización (OV) o de dominio (DV) se caracterizan por un pequeño candado verde en la barra de direcciones.

Certificados de validación extendida (Extended Validation Certificates)

Es el certificado que ofrece el mayor nivel de autenticación. A diferencia del OV, además de que sólo lo puede asignar una autoridad de certificación autorizada. Este realiza un análisis detallado de todos los aspectos importantes de la seguridad; por ende, es el tipo de certificado más caro, más confiable y con más credibilidad.

Es adecuado para páginas web que recopilan datos confidenciales importantes, como por ejemplo cuentas bancarias.

Una página web que ha sido cifrada con un certificado EV se reconoce con un pequeño candado ubicado en un recuadro completamente verde en la barra de direcciones.

Página web sin certificado SSL: cuando una web carece de un certificado SSL, no aparece ningún tipo de indicación visual sobre una conexión segura y, dependiendo del navegador, aparecerá una advertencia de sitio no seguro.

Certificado SSL inválido: una página web cuyo certificado SSL ha caducado o es inválido, se puede reconocer con un candado de seguridad cubierto con un triángulo amarillo de advertencia en la barra de direcciones.

Un poco del funcionamiento SSL/TLS

El protocolo SSL/TLS se ubica entre la capa de aplicación y la capa de transporte, la cual se separa en dos capas: high layer subprotocol y TLS record subprotocol.

TLS record subprotocol: es la capa que va en conjunto con la de transporte. Se encarga de fragmentar los datos en bloques de 2^14 bytes la que luego es comprimida y encriptada, agregando un código de autentificación.

High layer subprotocol: este subprotocolo a su vez se subdivide en 4 subprotocolos:

1) Handshake protocol: permite la autentificación conjunta de cliente-servidor y tratar los métodos de cifrado a utilizar en la comunicación. Se hace uso de mensajes para realizar las distintas peticiones de los cuales se detallan los más usados:

-Client Hello: inicia un saludo con el servidor para el uso TLS incluyendo variados métodos de cifrado y compresion para que el servidor elija el más conveniente para la conexión.

-Server Hello: responde al saludo anterior introduciendo un solo método de cifrado junto con un método de compresión.

-Certificate: se introduce el certificado para que TLS pueda corroborar la autentificación del sitio web con el que se quiere conectar y dependiendo del tipo de certificado también conocer información de la empresa.

-Server Key Exchange: contiene los parámetros requeridos para que el cliente pueda realizar un cifrado simétrico con el servidor.

-Client Key Exchange: de manera similar al anterior se introducen las claves que el servidor necesita para generar los mensajes cifrados.

-Finished: este mensaje trae la confirmación de que el handshake fue realizado con éxito y que la comunicación está cifrada denotando que el protocolo siguiente ya comenzó a funcionar.

2) ChangeCipherSpec Protocol: este protocolo se dedica simplemente a avisar que el método de cifrado escogido ha sido activado, pero no se puede introducir el cifrado a un mensaje por lo que forma parte de un protocolo separado.

3) Alert Protocol: el campo se encarga de detectar problemas notificando su nivel de gravedad y el tipo de problema que presenta

4) Application Data Protocol: se encarga de encapsular los datos de la capa aplicación de manera que pueda ser recibida por la capa de transporte sin dificultades de lo realizado por los subprotocolos anteriores.

Demostraciones

Utilizando el programa Wireshark se tomaron muestras de mensajes que surgían al realizar un intento de introducirse a una página segura con contraseña (en este caso Facebook). Para distinguir los paquetes importantes se realizó un filtro con TCP. Las figuras 1, 2 y 3 corresponden al proceso en que se accede satisfactoriamente a Facebook mientras que la figura 4 muestra el caso al ingresar incorrectamente la clave de la cuenta.

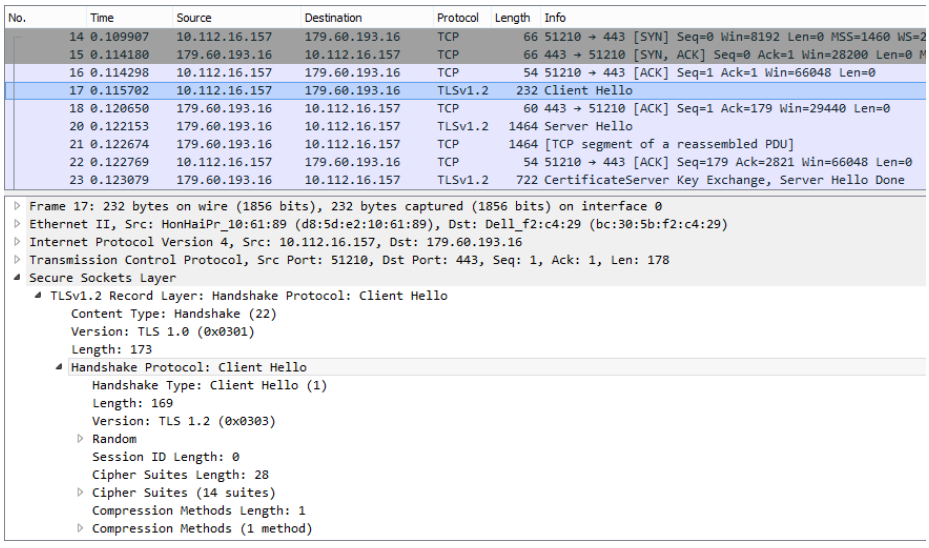

Figura1 – Inicio del handshake con el mensaje Client Hello

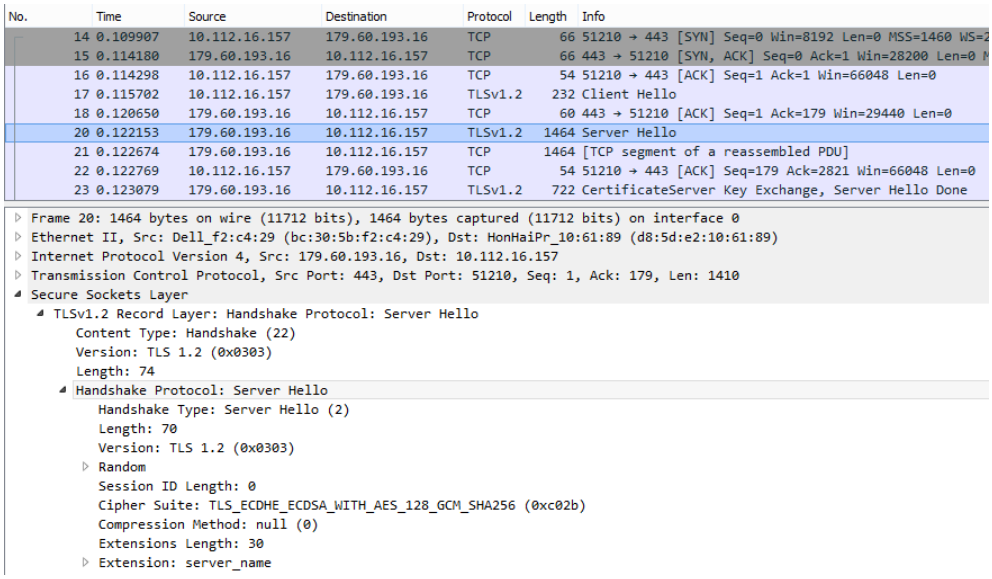

Figura2 – Respuesta del servidor mediante Server Hello

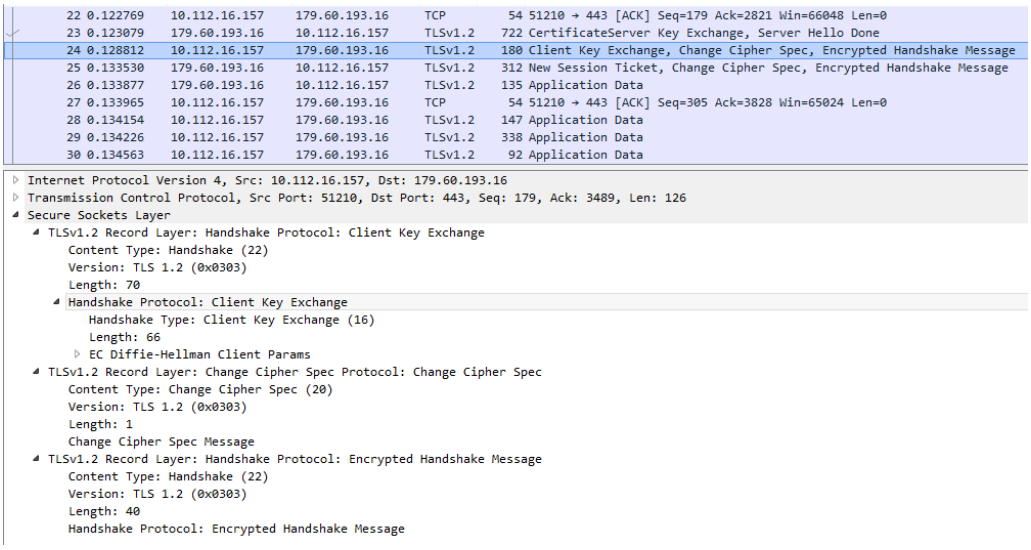

Figura3 – Finalización del handshake protocol y aviso de la encriptación del mensaje

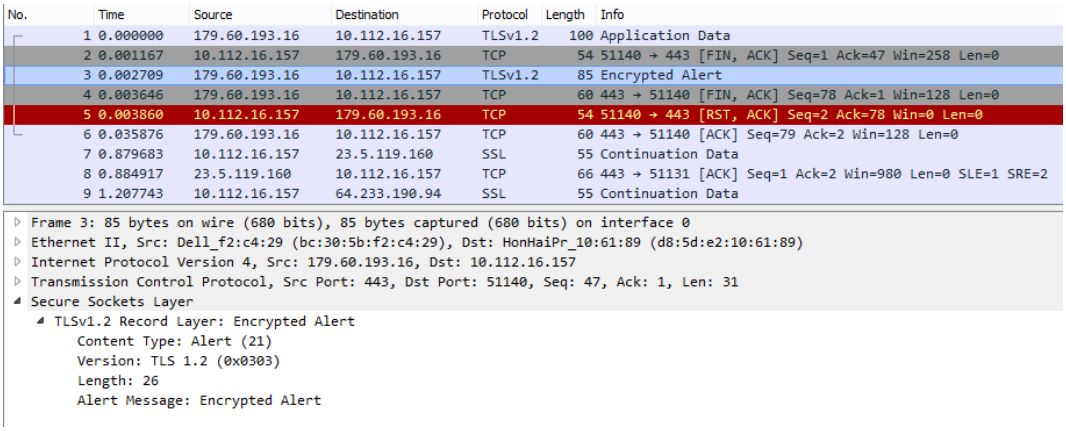

Figura4 – Intento fallido y mensaje de alerta del servidor

Se pueden presenciar elementos en común con lo explicado anteriormente como el contenido de los múltiples métodos de cifrado que en este caso son 14 puestos en el mensaje “Client Hello” junto con la elección del respectivo método de cifrado en “Server Hello”. En la figura 3 se realizan los intercambios de códigos y la finalización con el mensaje “Encrypted Handshake Message”.

Para el caso de la figura 4, al introducir mal la contraseña el servidor lo detecta y manda el mensaje Encrypted Alert anunciando problemas al momento de querer realizar la coneccion con cifrado, por lo que inmediatamente envía un mensaje al cliente anunciando un cierre de conexión al ser inseguro.

Conclusiones

Si no se certifica un sitio, se corre el riesgo de que sea un sitio “ficticio”, o que los datos sean vulnerables. Hay muchos sitios que requieren de una buena seguridad, como es el caso de los sitios bancarios. Para evitar dichas problemáticas, es una buena solución la adquisición de certificados para las páginas web que lo requieran, y que éstas utilicen el protocolo HTTPS.

Es probable que a futuro existan técnicas para vulnerar de manera más eficiente los actuales protocolos de seguridad, con lo que se podría mejorar dichos protocolos.

Bibliografías y Referencias:

https://www.1and1.es/digitalguide/paginas-web/creacion-de-paginas-web/certificados-ssl-y-https-maxima-seguridad-para-tu-web/

https://www.ssluniversal.com/faq/ssl/organization-validation-certificate

https://symantec.certicamara.com/centro-de-informacion/que-es-ssl-con-validacion-extendida-ev/

http://blog.fourthbit.com/2014/12/23/traffic-analysis-of-an-ssl-slash-tls-session