7) Qué es el Protocolo HTTPS?, ¿Cuáles son sus características? Ejemplifique

En la actualidad, **la seguridad y privacidad** al navegar por los sitios web, **se estima como una prioridad para todos los internautas**. Gracias a dicha necesidad global, **surgió el reconocido protocolo HTTPS o "Protocolo seguro de transferencia de hipertexto"** que proporciona un completo cifrado y autenticado a los usuarios de la red.

En vista de su notable potencia, muchas personas desean conocer, verdaderamente, **para que sirve este protocolo y cuáles son sus principales características**. Por lo que, en este post, especificaremos dicha información y, adicionalmente, mencionaremos **cuáles son sus mejoras y limitaciones, como funciona y por qué garantiza la mayor seguridad posible en la red**.

Si bien es cierto, **HTTPS** hace referencia a un protocolo de aplicación que está destinado a la transferencia segura de datos de hipertexto y se basa en el protocolo HTTP, pero **es la versión segura de este**. Así, consiste en un protocolo que ofrece la posibilidad de **establecer una conexión fiable entre el cliente y el servidor** con el objetivo de **evitar cualquier intercepción por parte de personas no autorizadas**.

En tal sentido, el **Protocolo Seguro para la Transferencia de Hipertexto** opera como un tipo de conexión que **sirve para encriptar los datos de los usuarios**. Gracias a esto, las personas que navegan en la red **podrán obtener un intercambio de datos completamente encriptado**, en vista de que el servidor estará autenticado.

En cuanto a su funcionamiento, básicamente, cuando un usuario confirma una entrada de URL en la barra de direcciones con la tecla Enter o, en su defecto, hace clic en un enlace; **el navegador establece una conexión de forma automática**. A continuación, con el uso del protocolo **HTTPS,** el servidor presenta un certificado que lo autentica como **un proveedor confiable**. Después, el usuario podrá verificar dicha autenticidad y con ello, **enviará una clave de sesión que solo será leída por el servidor**; sin la intercepción de un tercero.

Dado su funcionamiento, la principal particularidad del famoso **protocolo HTTPS**, radica en que **se ocupa de crear un canal seguro sobre una red**

insegura, básicamente. Con ello, logra proporcionar una protección contra diferentes tipos de ataques o amenazas, para garantizar que el servidor sea verificado y resulte de confianza.

Por su parte, de forma técnica, el Protocolo Seguro para la Transferencia de Hipertexto, contempla las siguientes características de sumo interés:

- Emplea un cifrado basado en la seguridad de textos SSL/TLS con el objetivo de crear un canal encriptado pertinente para el tráfico de información sensible. Considerando que, el nivel de cifrado dependerá del servidor remoto y el navegador usado.
- Por suerte, su utilización no requiere ninguna instalación de software adicional. Como consecuencia, puede ser empleado por cualquier usuario y sin restricción alguna. Lo cual, inspira confianza en los clientes potenciales, debido a la autenticación que realiza con un certificado.
- El protocolo HTTPS también se caracteriza por mostrar una óptima integración con los principales navegadores web, tales como: Google Chrome, Mozilla Firefox, Opera, Safari e Internet Explorer.
- Generalmente, este protocolo de seguridad se distingue a partir de un icono de candado que se encuentra en la parte derecha de la barra de direcciones. De esa forma, permite identificar páginas web confiables. Considerando que, además, también incluye el término "https" al inicio de la dirección URL.
- El contenido que se transmite con conexiones HTTPS, no puede ser almacenado en caché. Esto, para algunas personas puede ser ventajoso y para otras, un punto en contra.
- Para poder preparar un servidor web, en términos de configuración, para que admita conexiones HTTPS; el administrador tendrá que crear un certificado de clave pública para el servidor web.
- Un protocolo HTTPS puede ser vulnerado cuando se aplica a contenido estático de publicación disponible.
- En caso de que un infiltrado o una persona no confiable logre capturar los datos trasmitidos a partir del protocolo HTTPS, igualmente no podrá descifrar la información en cuestión porque está totalmente encriptada.

El antiguo HTTP consiste en un protocolo que permite realizar una petición de datos y recursos, por lo que se considera la base de cualquier intercambio de datos en la web. Sin embargo, a lo largo del tiempo, ha sido señalado como un protocolo muy fácil de violentar porque simplifica, para todas aquellas personas infiltradas, la captura de datos que se están transmitiendo.

Como consecuencia, se creó el protocolo HTTPS con el objetivo de **cambiar la funcionalidad del protocolo HTTP y proporcionar una mayor seguridad**.

Puesto que, el **Protocolo Seguro** para la Transferencia de Hipertexto hace uso de un cifrado en el que los infiltrados **no logran descifrar la información**, aun y cuando puedan capturar la transmisión de la misma. Pues, **se mantiene encriptado en su totalidad**. Por lo tanto, la principal diferencia entre el protocolo HTTP y HTTPS, **radica en la seguridad que proporcionan**. Tomando en cuenta que, este último emplea la misma tecnología que el antiguo HTTP, pero **incluye encriptación SSL**.

Sumado a ello, se observan las siguientes distinciones:

- En el protocolo **HTTP** las direcciones **URL** inician con **"http://"**. Mientras que, en el **HTTPS,** dichos enlaces empiezan con **"https://"**.
- Generalmente, el protocolo **HTTP** usa **el puerto 80**, por omisión. En cambio, los **HTTPS** utilizan **el puerto 443**.
- A diferencia del **HTTP** que **está sujeto a ataques man-in-the-middle y eavesdropping**, por lo que permiten que las personas malintencionadas adquieran acceso a cuentas de un sitio web, bancos e información confidencial; el **HTTPS** se encuentra diseñado para **soportar y resistir dichos ataques**, por lo que resulta más seguro.
- Regularmente, el **HTTP opera en la capa más alta del Modelo OSI**. Sin embargo, el protocolo **HTTPS** opera en una subcapa más baja para **garantizar el cifrado de un mensaje HTTP previo a la trasmisión** y descifrar los datos, una vez recibidos.

Los **datos enviados a través de un protocolo HTTPS** están asegurados gracias a un protocolo conocido como **"Transport Layer Security"** o **"TLS"** que, por defecto, **proporciona tres capas de protección primordiales** y así, determina el funcionamiento del protocolo **HTTPS** mejorado.

Dichas capas de protección de red, son las siguientes:

Cifrado

Por lo general, siempre que un equipo emite un mensaje desde el navegador web hacia el servidor web, existe la posibilidad de que **la información sea capturada por alguien que está tratando de interceptar el canal de comunicación**, con el fin de espiar todo el tráfico.

No obstante, el protocolo HTTPS se encarga de cifrar los datos de intercambios y los mantiene seguros ante miradas indiscretas. Gracias a esto, mientras el usuario esté navegando en un sitio web, ninguna otra persona podrá espiar sus movimientos ni realizar un seguimiento de sus actividades con el objetivo de usurpar su información confidencial. Más bien, la comunicación con el servidor web se hará efectiva de forma segura a partir de un cifrado de punto a punto.

Integridad

Así como existen riesgos de seguridad con los que se puedan perder los datos, también es posible que el mensaje transmitido desde el navegador web hasta el servidor sea capturado con el fin de cambiar la información que hay en él. Por lo que, una vez modificado, se enviará al destinatario y así, afectará la integridad del emisor.

Pero, por suerte, el protocolo HTTPS se ocupa de garantizar la integridad de los datos para que no puedan ser dañados ni modificados durante el proceso de transferencia, independientemente de que haya sido intencional o no. Esto significa que, bajo cualquier circunstancia, el mensaje llegará al receptor exactamente como se envió, sin riesgos a reducir su integridad.

Autenticación

El protocolo HTTPS también provee un gran nivel de autenticación, de forma que, logra proteger a los usuarios en contra de diferentes ataques. De tal modo, construye la confianza de las personas al suministrar páginas web que sean completamente auténticas.

Lo cual, ha sido verificado previamente, conociendo la identidad de quien ha enviado el mensaje por medio del uso de una firma digital. Por su parte, cabe acotar que, esta ventaja la consigue por medio de los certificados SSL, con los que se puede afirmar que estás conectado al lugar correcto. Tomando en cuenta que, por defecto, un certificado SSL es el encargado de mostrar que el navegador web es válido y que ha sido presentado por una autoridad de certificación legal.

Limitaciones

A pesar de que el protocolo HTTPS mejorado presenta numerosos beneficios a los usuarios, lo cierto es que también tiene algunos puntos en contra que vale la pena tomar en cuenta.

Por consiguiente, a continuación, nombramos cuales son las principales limitaciones o desventajas del HTTPS:

- Por defecto, el nivel de protección depende de la exactitud de la implementación del navegador web y los algoritmos de cifrado soportados. Por lo que, al no ser independientemente, podría presentar ciertas brechas en términos de privacidad.
- A partir de las conexiones HTTPS, es imposible almacenar el contenido en memoria caché. Lo cual, resulta desfavorable para diversos usuarios.
- Se ha evidenciado que, el protocolo HTTPS exhibe vulnerabilidad una vez se aplica a contenido estático de publicación disponible. Lo cual, facilita acciones no fidedignas por parte de usuarios no confiables que buscan tener acceso al texto plano y al texto cifrado. Esto, sirve para un ataque criptográfico.
- Otro punto débil radica en un menor rendimiento, como resultado del empleo del cifrado SSL. Puesto que, por naturaleza, el servidor tendrá que hacer numerosos cálculos y con ello, incrementa el tiempo de espera para dar respuesta.
- Desafortunadamente, los hosts virtuales no funcionan con el protocolo HTTPS. Pues, los servidores SSL solamente logran presentar un certificado, de manera estricta, para una combinación de Puerto/IP en particular.
- Los cargos adicionales por certificados pueden ser distintamente altos y, aparte, revela costes crecientes debido al aumento del tráfico. Por ende, las tarifas pueden llegar a ser muy altas en sitios web nuevos y pequeños, más que todo.

Seguridad

A pesar de que el protocolo HTTPS garantiza el cifrado en la transmisión de datos, en realidad no es tan seguro como parece. Pues, con las diferentes amenazas que operan en la red actualmente, el símbolo de seguridad de dicho protocolo no logra garantizar que una página web esté protegida en su totalidad. Considerando que, en este momento, los sitios maliciosos utilizan cada vez más HTTPS (sobre todo, los de phishing). Esto se debe a que, una conexión segura no es equivalente a un sitio seguro.

En otras palabras, se destaca que, a pesar de que el protocolo HTTPS cifra la información que es transmitida entre el sitio y tú, no tiene nada que ver con la seguridad del sitio web en concreto. Puesto que, un sitio malicioso podrá conseguir un certificado de este tipo sin problemas y cifrar todo el tráfico que se produce entre la página y tú para que no existan fisgones de por medio. No obstante, aunque aseguren que nadie más puede espiar los datos que suministras, tu contraseña e información confidencial estará en manos de dichos sitios.

Por lo tanto, podrá ser usurpada desde allí. Es decir, desde una web falsa o insegura. Como conclusión, la presencia del candado correspondiente al protocolo HTTPS, simplemente indica el uso de un certificado que garantiza un tráfico seguro y libre de las miradas de terceros. Sin embargo, dicho protocolo no emite avisos en torno a la inseguridad que contenga un sitio HTTPS malicioso que puede estar manipulado por estafadores online.