Journal **TechInnovation**
Volumen 1, Número 2, 2022
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO ORIGINAL

Aplicación de protocolos SSL y TSL para él envió de información

Application of SSL and TSL protocols for the sending of information

https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.4-9

Recibido: 15-04-2022 **Aceptado:** 27-06-2022 **Publicado:** 31-07-2022

Geanfrank Isaias Cruz Lucas[1]
https://orcid.org/0000-0002-0881-6499

Rolando Euclides Galarza Espinoza[2]
https://orcid.org/0000-0002-3405-2357

Ronald Steven Delgado De La Cruz[3]
https://orcid.org/0000-0002-6819-3481

Mario Javier Marcillo Merino[4]
https://orcid.org/0000-0001-5818-367X

1. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa – Manabí – Ecuador. cruz-geanfrank0339@unesum.edu.ec
2. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa – Manabí – Ecuador. galarza-rolando1517@unesum.edu.ec
3. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa – Manabí – Ecuador. delgado-ronald0502@unesum.edu.ec
4. Ingeniero en Sistemas, Magister en Docencia Universitaria. Docente titular de la Universidad Estatal del Sur de Manabí. Jipijapa – Manabí – Ecuador. mario.marcillo@unesum.edu.ec

Volumen: 1
Número: 1
Año: 2022
Paginación: 10-21
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/13
***Correspondencia autor:** cruz-geanfrank0339@unesum.edu.ec

RESUMEN

Durante muchas décadas se ha escuchado sobre el robo de información vía internet y no es para menos debido a que los datos de cada usuario se encuentran en contante peligro y es aquí donde se puede muchos se preguntan si existe, alguna forma segura de poder navegar por internet sin correr el riesgo de que me roben información. Se debe tener presente que los protocolos criptográficos se utilizan para encriptar los datos que se envían y a su vez autentica una conexión segura cuando se navega en la web, por tal razón si se habla de alguna forma segura para navegar por internet la respuesta principal seria sí aplicando los protocolos SSL y TSL para él envió de datos. Por otro lado si se utiliza una tarjeta de crédito para realizar pagos en cualquier sitio web y este no utiliza protocolos encriptados lo recomendable es no ingresar los datos personales de la tarjeta porqué el objetivo principal es aplicar el envió de datos o información mediante los protocolos criptográficos, en el caso de no ser utilizados se corre el riesgo que la información proporcionada en el sitio web pueda caer en manos de agentes maliciosos, piratas informáticos o Ciberdelincuentes, existen estudios que demuestran que el usar protocolos criptográficos mejora la experiencia de navegación y se podría comparar como el navegar por sistemas operativos seguros como lo es Kali Linux, su experiencia de navegación es completamente segura y los datos ingresados en sus aplicaciones tienen seguridad de punto a punto.

Palabras clave: Certificación HTTP; Modus Operandi; Protocolos Criptográficos.

ABSTRACT

For many decades we have heard about the theft of information via the Internet and it is not for less because the data of each user is in constant danger and it is here that many wonder if there is any safe way to navigate through internet without running the risk of information being stolen. It should be borne in mind that cryptographic protocols are used to encrypt the data that is sent and in turn authenticate a secure connection when browsing the web, for this reason if there is any safe way to browse the internet, the main answer would be yes. applying the SSL and TSL protocols for sending data. On the other hand, if a credit card is used to make payments on any website and it does not use encrypted protocols, it is advisable not to enter the personal data of the card because the main objective is to apply the sending of data or information through cryptographic protocols. If they are not used, there is a risk that the information provided on the website may fall into the hands of malicious agents, hackers or cybercriminals. There are studies that show that using cryptographic protocols improves the browsing experience and could Compare how to browse secure operating systems such as Kali Linux, your browsing experience is completely safe and the data entered into your applications have end-to-end security.

Keywords: Cryptographic Protocols; HTTPS Certification; Modus Operandi.

Introducción

En la actualidad, la seguridad en el envío de información es esencial para garantizar la privacidad y la confidencialidad de los datos transmitidos a través de internet. Según el Instituto Nacional de Standards and Technology (NIST), "la seguridad en las comunicaciones es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de redes públicas o privadas" (PowerData, 2022). Para lograr esto, existen diversos protocolos de seguridad que se utilizan para encriptar la información durante su transmisión, evitando que terceros no autorizados accedan a ella. Uno de los protocolos más utilizados son el SSL (Secure Sockets Layer) y el TLS (Transport Layer Security).

El protocolo SSL fue desarrollado originalmente por Netscape en 1994 y se utilizó ampliamente en la transmisión segura de información en sitios web y correo electrónico. Sin embargo, en 1999 fue reemplazado por el protocolo TLS, el cual es considerado como una evolución del SSL y ofrece mayores medidas de seguridad. Según el experto en seguridad informática, Bruce Schneier, "TLS es el estándar de la industria para la seguridad de las comunicaciones en internet, y es ampliamente utilizado en aplicaciones como el correo electrónico, la navegación web y las transferencias de archivos" (Cloudflare, 2023)

Los protocolos SSL/TSL, son más usados para compañías y organizaciones, lo cual quieren brindar una comunicación más segura, es decir los navegadores.

Acorde con perspectivas de (LIBERATO, 2019), hace mención en su proyecto de titulación de que los protocolos no afectan en el rendimiento de los sitios web, por lo contrario, demuestra que mejora la seguridad para la comunicación de HTTP, se menciona que el manejo de información va hacer más seguro sin que logren robar la fuente de datos de las compañías, como también la información de los clientes.

Acorde con perspectivas de (Rendón & Mendoza, 2020) mencionan un caso de estudio el cual demuestra que cuando se unen los protocolos SSL/TSL provee confidencialidad, integridad aplicando la criptografía, a las aplicaciones que envían datos a través de internet, la aplicación de estos protocolos se dan en conjunto solo para la mejora de la seguridad en la web, muchos investigan sobre la vulnerabilidad de los protocolos, como también fue evaluar la seguridad de información, sin olvidar que se centran en métodos de autenticación principalmente en los servidores.

En este artículo se analizará la aplicación de los protocolos SSL y TLS en el envío de información, con el objetivo de comprender su funcionamiento y las ventajas que ofrecen en términos de seguridad. Se discutirán aspectos como cómo se realiza la encriptación de la información, las diferencias entre los dos protocolos y su compatibilidad con diferentes dispositivos y sistemas operativos. También se explorarán las implicaciones legales y normativas en torno a su uso, como por ejemplo la normativa de la Unión Europea (UE) sobre el Reglamento General de Protección de Datos (RGPD) y se proporcionarán recomendaciones para garantizar la seguridad de la información enviada a través de internet.

Además, se realizó un análisis histórico-lógico del desarrollo de ambos protocolos, para entender cómo han evolucionado y se han adaptado a las necesidades de seguridad actuales. También se utilizará el análisis-síntesis para comparar y contrastar las ventajas y desventajas de cada protocolo, y el método bibliográfico-documental para recopilar información de fuentes confiables y estudios relevantes

Desarrollo

Los protocolos SSL (Secure Sockets Layer) y TLS (Transport Layer Security) son dos de los métodos más comunes utilizados para

garantizar la seguridad de las comunicaciones en internet. Ambos protocolos proporcionan una conexión segura entre un servidor web y un navegador mediante el uso de certificados digitales y cifrado de datos.

SSL fue desarrollado originalmente por Netscape en 1994 y se utilizó ampliamente durante muchos años para garantizar la seguridad de las transacciones en línea (Soluciones Simples En TI, 2023). Sin embargo, en el año 2000 se descubrieron vulnerabilidades en el protocolo, lo que llevó a su reemplazo por TLS. Aunque SSL ya no se utiliza comúnmente, muchos sitios web aún utilizan "SSL" en su nombre de dominio como, por ejemplo, "https://www.facebook.com", como una forma de indicar que utilizan una conexión segura. Sin embargo, en realidad están utilizando TLS.

TLS es una actualización de SSL y se ha convertido en el estándar de facto para la seguridad de las comunicaciones en internet. El protocolo proporciona una capa adicional de seguridad mediante la utilización de algoritmos de cifrado más avanzados y la verificación de la identidad del servidor mediante certificados digitales (Amazon Web Services, 2023).

Para aplicar un protocolo SSL o TLS, un sitio web debe obtener un certificado digital de una autoridad de certificación (CA) reconocida. El certificado contiene información sobre el propietario del sitio web, así como una clave pública que se utiliza para cifrar la información transmitida. Cuando un usuario accede a un sitio web que utiliza SSL o TLS, su navegador verifica la validez del certificado y establece una conexión segura utilizando la clave pública del certificado.

Además de proporcionar seguridad en las transacciones en línea, SSL y TLS también se utilizan para garantizar la privacidad de las comunicaciones de correo electrónico y la seguridad de las conexiones VPN. Los certificados digitales también se utilizan para garantizar la autenticidad de las aplicaciones móviles y para proteger la privacidad de las comunicaciones en aplicaciones de mensajería.

Se puede decir que, los protocolos SSL y TLS son esenciales para garantizar la seguridad de las comunicaciones en internet. Ambos protocolos utilizan certificados digitales para autenticar al servidor web y cifrar la información transmitida. Aunque SSL ya no se utiliza comúnmente, muchos sitios web aún indican que utilizan una conexión segura utilizando el término "SSL" en su nombre de dominio, en realidad están utilizando el protocolo TLS.

Metodología

Los métodos utilizados en la presente investigación fueron principalmente las fuentes bibliográficas lo mismo que conllevo a una investigación completa y con bases sólidas. Por otro lado, los métodos utilizados fueron análisis-síntesis, bibliográfico-documento, histórico-lógico al utilizar metodologías en conjunto se puede obtener una comprensión más completa del tema como, por ejemplo:

El método de análisis-síntesis se utilizó en el análisis del protocolo SSL y del TSL, comprendiendo las ventajas, desventajas, características y funcionalidades de los mismos.

El método bibliográfico-documental permitió la recopilación y análisis de fuentes a través de libros, artículos científicos y tesis, entre otros documentos que brindaron su información relevante sobre los protocolos SSL y TLS, el análisis, la sistematización, comparación e interpretación ayudaron a obtener una información precisa sobre los protocolos criptográficos.

El método histórico-lógico se utilizó en la búsqueda de los antecedentes investigativos referente al origen y la evolución de los protocolos SSL y TSL.

Resultados

Si se utilizan los protocolos SSL y TLS para el envío de información, se espera que obtengas los siguientes resultados:

- Protección de la privacidad: Los protocolos SSL y TLS utilizan cifrado para proteger la privacidad de la información transmitida. Esto significa que solo las partes autorizadas podrán acceder a la información, lo que previene la interceptación o el robo de datos.
- Integridad de los datos: Los protocolos SSL y TLS también verifican la integridad de la información transmitida, lo que significa que detectan y evitan cualquier modificación no autorizada de los datos.
- Autenticación: Los protocolos SSL y TLS utilizan certificados digitales para autenticar las partes que se comunican, lo que garantiza que solo se está comunicando con el destinatario esperado.
- Mayor confianza y seguridad para los usuarios: Al utilizar protocolos SSL y TLS, los usuarios tendrán mayor confianza en la seguridad de sus comunicaciones y transacciones en línea, lo que podría mejorar la experiencia del usuario y aumentar la confianza en la marca.
- Mejora en la conformidad: Al utilizar protocolos SSL y TLS, también se cumplen los estándares y regulaciones de seguridad de la información, lo que puede ayudar a cumplir con las regulaciones legales y de cumplimiento.

Según el estudio realizado por (Raul Bareño - Gutiérrez, s.f.) se demostró que los protocolos de SSL/TLS sirven para mejorar la información por la web, en este caso se demostró que en base a un sistema creado para votaciones electrónicas con características de seguridad SSL y TSL.

Tabla 1. Uso de los protocolos.

Escenario Propuesto	ESC 1 TLS	ESC 2 TLS	ESC 2 IPSEC	ESC 3 TLS e IPSEC
Tiempo	26	35	20	38
Paquetes enviados PC1	114	239	263	290
Paquetes Recibidos BD	114	245	255	297
% Ocupación del canal PC1	2,4	1,227	1,227	2,3124
% Ocupación del canal BD	2,3	1,021	1,021	3,7
% Procesamiento en PC1	5,2	2,9	5,1	8
% Procesamiento en BD	6,1	4,1	6,4	6
% Disponibilidad del canal	97,7	99,977	99,97	96,3

En la tabla se demostró las características de SSL/TLS e IPSEC para el prototipo e-vote, inclusive se muestra que los resultados de haber utilizado los protocolos fueron mejores para el manejo de una buena seguridad de información.

Por otro lado, la revista ibérica de sistemas y tecnologías de información menciono que los protocolos sirven para un mejor funcionamiento a través de una configuración en sistemas como Ubuntu server para la encriptación.

Tabla 1. Configuración en sistemas como Ubuntu server.

Equipo	Puertos abiertos encontrados	
	Implementacion 1 (Ubuntu Server)	Implementacion 2 (Windows Server)
Servidor	1	12
Cliente Windows	4	4
Cliente Linux	1	1

Acorde a este resultado se logró determinar que el uso del protocolo SSL y el protocolo TSL son más seguros juntos para mejor seguridad de información tanto como en el usuario y el navegador.

Conclusiones

En conclusión, los protocolos SSL y TLS son fundamentales para garantizar la seguridad de las comunicaciones en internet. Ambos protocolos utilizan certificados digitales y cifrado de datos para proteger la privacidad y la integridad de la información transmitida. Aunque SSL ya no se utiliza comúnmente, TLS se ha convertido en el estándar de facto para la seguridad en las comunicaciones en internet y se usa en una variedad de aplicaciones, como transacciones en línea, correo electrónico, conexiones VPN y aplicaciones móviles.

Bibliografía

Amazon Web Services. (26 de Enero de 2023). Obtenido de https://aws.amazon.com/es/what-is/ssl-certificate/

Cloudflare. (26 de Enero de 2023). Obtenido de https://www.cloudflare.com/es-es/learning/ssl/transport-layer-security-tls/

LIBERATO, E. E. (2019). Repositorio Institucional. Obtenido de http://repositorio.unas.edu.pe/handle/UNAS/1535

PowerData. (20 de Noviembre de 2022). Obtenido de https://www.powerdata.es/seguridad-de-datos

Raul Bareño - Gutiérrez, S. E.-U.-N.-P. (s.f.). web.archive.org. Obtenido de web.archive.org: https://web.archive.org/web/20220803011842id_/https://revistas.uis.edu.co/index.php/revistauisingenierias/article/download/5014/9473?inline=1

Rendón, A. Z., & Mendoza, M. N. (mayo de 2020). Revista Ibérica de Sistemas e Tecnologias de Informacion. Obtenido de https://www.proquest.com/openview/5cb3dc0d41d9ef45f370b8ee509d3c43/1?pq-origsite=gscholar&cbl=1006393

Soluciones Simples En TI. (26 de Enero de 2023). Obtenido de https://acortar.link/GAhcqs

Cómo citar: Cruz Lucas, G. I., Galarza Espinoza, R. E., Delgado De La Cruz, R. S., & Marcillo Merino, M. J. (2022). Aplicación de protocolos SSL y TSL para él envió de información. Journal TechInnovation, 1(2), 4–9. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.4-9