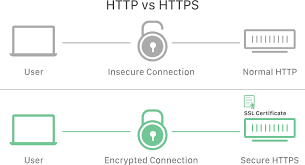
Secure Sockets Layer (SSL) is a protocol that keeps internet connections secure. It does this by protecting information from being stolen as its transferred from one system to another system. These systems could be clients or servers. For example, when you access your Gmail you are accessing a web server as a client of that web server. When sending and receiving emails there is a good chance SSL is being used to secure the connection and protect the information being transferred. Although SSL has been replaced by Transport Layer Security (TLS). TLS isn’t much different from SSL, and simply replaced SSL and has some improved security features.

Security when using the internet is very important. When sending messages, emails and accessing files over the internet you are very vulnerable to cyber security threats. Your data such as personal information and email/message history can be broken into by hackers during transport. Your emails and messages and account information can contain your name, age, address, postal code and even your credit card information. That’s where TLS comes in. It helps to protect your data and information from cyber security threats. You can tell the website your accessing is secured by TLS by the padlock symbol beside the website URL. This means the website is using Hypertext Transport Protocol Secure (HTTPS). This is the secure version of Hypertext Transport Protocol (HTTP). The secure version uses TLS to secure web communications.

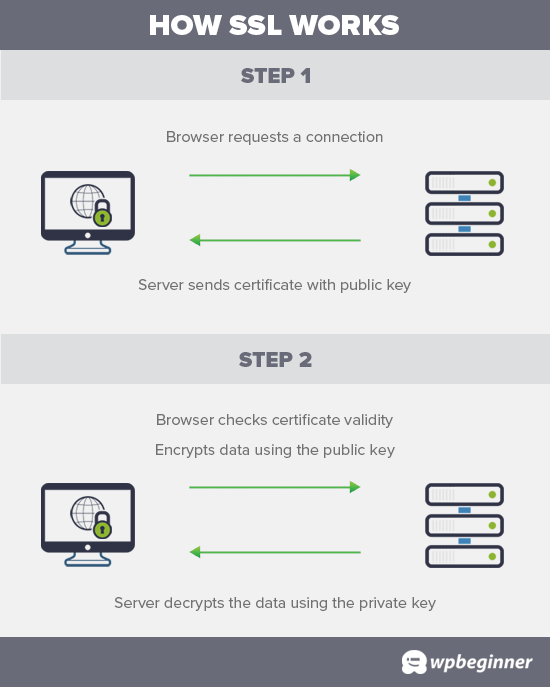
Hypertext Transport Protocol (HTTP) vs Hypertext Transport Protocol Secure.

<https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.cloudflare.com%2Flearning%2Fssl%2Fwhat-is-ssl%2F&psig=AOvVaw0-2ukdYyeGEwAab-K56v_2&ust=1633572761099000&source=images&cd=vfe&ved=0CAsQjRxqGAoTCNiel_PatPMCFQAAAAAdAAAAABCIAQ>



Encryption is the main thing protecting your data. Encryption is when normal text also called plaintext is encrypted and turned into ciphertext. Encryption can come in many different forms and types. For example, they can vary in key size which is the length of the encryption. Common key sizes can range from 128 bits to 256. The more bits the better the encryption. Just like any other form of physical or technological security. For example, a lock that has 8 numbers or letters has many more possible combinations than one with only 4 numbers or letters. So, 256-bit encryption has more possibilities than 128-bit encryption and therefor is much more secure. TLS currently only supports key sizes ranging from 128 bits to 256 bits. Although 128-bit encryption is very secure and takes a lot of computational power to decrypt.

Another thing that SSL/TLS uses are SSL Certificates. SSL are digital certificates which are bound to cryptographic keys. These keys are then used to secure sessions between a user (client) and the web server. For the browser to trust the certificate is must have the same URL of the website using it, be issues by a legitimate Certificate Authority (CA) and not be expired. So, a digital certificate is basically a websites identification almost like a driver’s license. It identifies the website and identifies that it’s a secure website. The reason these certificates are given by Certificate Authorities which are trusted organizations. These organizations make sure that sites are secure and that online interactions can be done securely.



How SSL works using encryption and certificates.

<https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.wpbeginner.com%2Fglossary%2Fssl%2F&psig=AOvVaw0-2ukdYyeGEwAab-K56v_2&ust=1633572761099000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCNiel_PatPMCFQAAAAAdAAAAABAF>

In conclusion, when using the internet and accessing various websites, it’s a good idea to search for the padlock icon beside the URL. It isn’t do or die, but it helps to secure your personal information and make your online interactions private.

Sources

Parms, J. (2021, June 23). *SSL vs. TLS - what are differences?* SSL2BUY Wiki - Get Solution for SSL Certificate Queries. Retrieved October 5, 2021, from https://www.ssl2buy.com/wiki/ssl-vs-tls.

*What is HTTPS? | cloudflare*. Cloudflare. (n.d.). Retrieved October 5, 2021, from <https://www.cloudflare.com/en-ca/learning/ssl/what-is-https/>.

Admin. (2020, December 8). *What is a certificate authority?* GlobalSign GMO Internet, Inc. Retrieved October 5, 2021, from https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies.

*What is SSL, TLS and HTTPS?* DigiCert. (n.d.). Retrieved October 5, 2021, from https://www.websecurity.digicert.com/en/ca/security-topics/what-is-ssl-tls-https.