SSL / TLS and HTTPS?

What is SSL / TLS and HTTPS?

You have heard of all these terminologies and what do they all mean? How do they work together to provide a more secure way of browsing your web on the internet?

In this article, I will explain all the basics that you will need to know about SSL / TLS and how that is used to build the secure HTTP protocol that we are using in our modern day.

HTTP - Time before secure internet

In the beginning, there is the plain old HTTP, the hypertext transfer protocol. RFC 1945 explains the hypertext transfer protocol and how it is used to share HTML documents between servers and clients. When HTTP is invented it was used purely for sharing documents between users. I.e. a research paper that can be shared in HTML document to other university around the world. Security was not a concern back then because there was no need to secure any of the content if it was meant to be shared freely around the world.

However, the surge in online banking and online shopping in the 1990s increase the concern of security. When form logins can be easily intercepted and the user name and password can be recorded down because with HTTP those information are in plaintext, thus a more secure way of browsing the web was needed.

HTTPS is created, it is HTTP wrapped in SSL / TLS, which essentially encrypt the data that's transferred between the client and server, making it difficult for anyone sniffing the TCP packets in the internet hard to decode what information is shared.

SSL / TLS Why two names?

Let's get the elephant out of the room first why is there two different name for the same thing?

SSL = Secure socket layer

TLS = Transport layer security

TLS is the direct successor to SSL, as all version of SSL is now all deprecated. They are both communication protocols that encrypts the data between servers and clients.

We still refer as SSL because it is commonly understood compared to TLS acronym.

To use SSL / TLS we will need to create what's called SSL certificate which verifies the server's identity and verifies the integrity if the encryption data.

HTTPS

Now HTTPS is just HTTP but with SSL / TLS layer on top of it. Between the server and client it will use HTTP to do the communication, but the transportation of the actual TCP packet is done through SSL connection.

To use HTTPS connection the server and the client establish the SSL connection first. To do that the server and client first do a SSL handshake to find which cipher they will want to use. Then certificate from the server is validated with the client. Finally key exchange is performed to do the actual encryption of the data.

To recap quickly:

1. SSL Handshake, exchange the cipher suite information, agree on which cipher suite to use for the duration of the SSL connection
2. Certificate exchange, the server have to prove the identity to the client by sending over it's certificate. The client will then verify the certificate by going through the certificate chain of trust.
3. Key exchange, then key exchange is perform in order to use it to encrypt the data

In the next section we will go over how to generate a server certificate, sign it, and validate it.

Revision #1
Created 2024-01-07 20:35:59 UTC by Tamarine
Updated 2024-01-07 22:09:18 UTC by Tamarine