What is TSL/SSL?

Transport **L**AYER **S**ecurity (TSL) is a cryptographic protocol that is used to secure end-to-end communication over networks by encrypting the data so that unauthorized third parties (e.g. hackers) are unable to see what is being transmitted (Internet Society, n.d.). **S**ecure **S**ocket **L**ayer (SSL) is the deprecated predecessor of TSL. TLS version 1.0 began development as SSL version 3.1, then the name was changed before publication because it was no longer associated with Netscape (CLOUDFLARE, n.d.).

How does it work?

There are three main components of TLS;

1) Encryption: hides the data being transferred from unauthorized third parties. A TLS connection is created using a sequence called TLS handshake which establishes a set of algorithms that specifies details such as which shared session keys will be used for that session. (CLOUDFLARE, n.d.).
   TLS uses both symmetric and asymmetric cryptography as it provides a good compromise between performance and security (Internet Society, n.d.).
   - In Symmetric cryptography: data is encrypted and decrypted with a shared key known to both the sender and recipient (Internet Society, n.d.). Since only one key is used, it is much less computationally intensive than asymmetric cryptography.
   - Asymmetric cryptography: is safer than symmetric cryptography because two keys are used instead of one. The public key is used to encrypt the data and the private key is used to decrypt it (Internet Society, n.d.). The keys are related by some complex mathematical formula that is difficult to decipher hence, it takes a lot of computing resources to achieve (Internet Society, n.d.).
2) Authentication: makes sure that the parties exchanging information are authorized parties. The server must prove its identity to the client using the public key (CLOUDFLARE, n.d.). Anyone can unscramble data encrypted with the private key to ensure its authenticity, but only the original sender can encrypt data with the private key (CLOUDFLARE, n.d.).
3) Integrity: verifies that the data has not been forged or tampered with (CLOUDFLARE, n.d.). After data encryption and authentication, the data is signed with a message authentication code which can be verified by the recipient to ensure integrity (CLOUDFLARE, n.d.).

Role of CAs

A **C**ertificate **A**uthority (CA) is a trusted third party that gives clients the assurance that they are connecting to a server operated by a validated entity (Internet Society, n.d.). HTTPS uses TLS encryption (CLOUDFLARE, n.d.). When a secured connection is made to a website through HTTPS, a public key certificate is sent from the server to the computer (Merrill, 2008). The certificate contains a digital signature that the computer uses to verify the identity of the site being connected to (Merrill, 2008).

Why is it a good idea?

TLS encryption protects web applications from data breaches and distributed denial-of-service attacks (CLOUDFLARE, n.d.). It also protects sensitive information such as login and credit card details from easily being collected by others (Internet Society, n.d.).

References

CLOUDFLARE. (n.d.). *What is Transport Layer Security (TLS)?* Retrieved from CLOUDFLARE: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

Internet Society. (n.d.). *TLS Basics*. Retrieved from Internet Society: https://www.internetsociety.org/deploy360/tls/basics/

Merrill, S. (2008). *MD5 collision creates Rogue Certificate Authority*. Retrieved from Tech Crunch: https://techcrunch.com/2008/12/30/md5-collision-creates-rogue-certificate-authority/