Security: SSL

Transport layer security is a security protocol to encrypt the communication between applications of different hosts, usually between web applications and servers. It evolved from SSL, Secure Socket Layer, which is propriety-associated with Netscape. (“What Is Transport Layer Security”)

A TLS connection is initiated with a handshake procedure, which uses asymmetric encryption to exchange randomly generated control data. It’s called asymmetric because the sender and the receiver use different keys. The random data is then used to create a new key, the session key, for the data encryption in the session. After the TLS handshake, both sides use the same session keys for encryption, which is called symmetric encryption. Session keys are temporary keys that are not used again once the session is terminated. A new, random set of session keys will be created for the next session. (“How Does SSL Work? | SSL Certificates and TLS”)

After the encryption procedure of TLS is introduced, it’ll be necessary to explain how this procedure ensures security. When both sender and receiver have the same key, they can use this same secret key to encrypt a message from “Hello” to “aB/NEJ4qe34” and decrypt a message from “aB/NEJ4qe34” to “Hello”. The secret key can be either a number, a word or a string of random letters. There are a lot of algorithm to achieve this purpose and the most widely used is AES-128, AES-192, and AES-256. The longer the key, the harder the key could be cracked (“Symmetric vs. Asymmetric Encryption – What are differences?”). It will take millions of years to crack 256-bit AES encryption with Tianhe-2 (MilkyWay-2), the fastest supercomputer in the world (Nohe, 2019).

The next question is then how to let sender and receiver have the same secret key. The physical exchange is too costly, and the internet exchange is not safe. Asymmetric encryption solves this dilemma and it is applied in the TLS handshake stage to exchange the secrete key. While a public key is known to anyone, a private key is only known to the send or receiver. On one hand, when the server uses the private key to decrypt, it’ll be the only one that can access the information. On the other hand, when the client uses the public key to send data, it’ll check certification authority (CA) to ensure that the public key is registered by the correct server. With asymmetric encryption, the secrete key itself is also exchanged in a secured way.

Normally asymmetric encryption needs to use longer key to reach the same security level as symmetric encryption. For instance, a 128-bit symmetric AES key is roughly equivalent to an asymmetric 3072-bit RSA key in terms of the actual security they provide. This is why the costly asymmetric encryption is only used in the handshaking stage.

Reference Material

“How Does SSL Work? | SSL Certificates and TLS.” *Cloud Flare*. Retrieved from: https://www.cloudflare.com/learning/ssl/how-does-ssl-work/. Accessed on Oct. 19, 2019.

Nohe, P. “How strong is 256-bit Encryption?” *Hashed Out*. May. 2, 2019. Retrieved from: https://www.thesslstore.com/blog/what-is-256-bit-encryption/.

“Symmetric vs. Asymmetric Encryption – What are differences?” *SSL2BUY*. Retrieved from: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. Accessed on Oct. 19, 2019.

“What Is Transport Layer Security?” *Cloud Flare*. Retrieved from: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/. Accessed on Oct. 19, 2019.