Natnael Kebede

Scenario Response

In the recent meeting with a vendor, the vendor used HTTPS (HyperText Transfer Protocol Secure), SSL (Secure Sockets Layer), and TLS (Transport Layer Security) interchangeably as the same thing. Security experts also use SSL when they’re referring to TLS (Aumasson, 2018). Indeed, these technologies are all related as their goal is to provide security. That is, both SSL and TLS perform the same essential function, which is to establish a secure communications channel between a client and server over an insecure medium such as the internet. However, even though they provide the same services which HTTPS takes advantage of, SSL, TLS, and HTTPS are somewhat different with different standards. The primary difference between SSL and TLS is that SSL refers to older communication protocols with versions that have security flaws. They are also incompatible with TLS versions. For example, SSL 3.0 doesn’t interoperate with TLS 1.0 (Morton, 2011). In terms of functionality, SSL uses asymmetric encryption and is commonly used in web browsers, email servers, or any communication between a client and server. For example, instant messaging servers might use SSL to protect the exchange of messages (“Differences between SSL and TLS,” n.d.). Another difference between the two protocols is that TLS is the successor of SSL and the latest industry-standard cryptographic control. The current version of it, TLS 1.3, is a secure, simple, faster, and a more efficient protocol compared to its previous versions and all versions of SSL. TLS also provides stronger confidentiality, integrity, and authentication compared to SSL by using robust encryption algorithms and efficient handshake protocol involving certificates. In terms of functionality, TLS also uses the same type of asymmetric encryption and is commonly used where SSL could be used. However, it is best known for 's' in HTTPS when compared to SSL. HTTPS is a protocol that is an application-specific implementation of SSL or TLS so that the security of exchanged data gets insured over the internet. However, all versions of SSL are currently considered insecure for modern use in HTTPS (“Technical Guidelines, n.d.). Hence, HTTPS uses TLS as a backbone to enable secure browsing in applications such as online banking by encrypting website connection so that data associated with user credentials, card numbers, and other sensitive information is protected from being exploited by an eavesdropper (Aumasson, 2018). A locked padlock in a browser also indicates the existence of a TLS session in HTTPS. In the absence of such a scenario, the website would be marked as NOT SECURE by the browser (“Technical Guidelines,” n.d.). Thus, as explained, there are differences between SSL, TLS, and HTTPS, even though the vendor interchangeably considered the terms the same.

References

Aumasson, Jean-Philippe. (2018). *Serious Cryptography*. San Francisco, CA: No starch press.

Differences between SSL and TLS. (n.d). *Indiana University Knowledge Base*. Retrieved from https://kb.iu.edu/d/anjv

Morton, B. (2011). Is it SSL TLS or HTTPS. *Entrust Datacard*. Retrieved from https://www.entrustdatacard.com/blog/2011/may/is-it-ssl-tls-or-https

Technical Guidelines. (n.d.). The HTTPS-Only Standard. Retrieved from https.cio.gov/technical-guidelines/.