Secure Web Communication Protocols in Brief

Joseph Patrick C. Galvez

American Military University

ISCC266: Cryptography Concepts

Mr. Joel Stewart

June 15,2025

Secure Web Communication Protocols in Brief

Ever since the internet was widely adopted during the 1990s, there has been a need for secure communications to safeguard transactions and interactions that take place within it. This is why SSL was developed in 1995 and later TLS in 1999 to provide security for the transport layer. Later on, IPsec was created to provide security for the network layer. These two protocols combined secure both traffic and networking information to secure both the transit of packets as well as to provide security for the network devices on which they travel on.

SSL or Secure Socket Layer is no longer in large-scale use due to the development of TLS or Transport Security Layer. TLS is a layer 4 protocol, meaning it deals with the transportation of packets in between networking devices. TLS has three subprotocols: The handshake, the change cipher spec, and the alert protocols according to Frank et at.(2005). The handshake initiates the interaction by telling the other device that the interaction will be cryptographic in nature and a shared key is agreed upon and works through a certificate exchange. The alert protocol ensures that any discrepancies are found and resolved, and the change cipher spec protocol is only found on TLS 1.0,1.1, and 1.2 (Frank et al.,2005). After a common key is established, a common cryptographic method is agreed upon, for example, AES. Other protections used by TLS include anti-replay protection and key management.

In contrast to TLS, IPSEC is a layer 3 protocol and it works by encrypting packets before they are sent. IPSEC does this by using protocols such as: AH, ESP, IKE, and IPComp (McKay and Cooper, 2019). AH or Authentication Header protects the header of the packet which contain the destination and sender of the packet. A more modern alternative to AH is ESP. ESP is much like AH but also provides protection for the trailer of the packet and is utilized in tunnel mode for more secure communications. IKE is a protocol that is used to validate keys and establish keys. This is done in either main mode or aggressive mode, aggressive mode uses three messages as opposed to main mode’s three pairs; it is less secure but it is faster. Finally IPComp can decide whether or not to compress a packet, it will not

compress a packet if it ends up being larger compared to not being compressed (McKay and Cooper, 2019).

In conclusion, having secure web communications requires security protocols in both layer 3 and layer 4. TLS/SSL is responsible for initiating secure communications as well as deciding which cryptographic methods to use. IPSEC secures layer 3 by encrypting the sender and receiver, as well as allowing for tunneling mode, establishing common keys, and the compression of packets if it is beneficial. Through these protocols, secure web communications are reliable and safe enough for sensitive transactions such as the transfer of confidential documents and financial transactions to take place.

References

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005, December 1). *Guide to IPsec VPNs* (NIST Special Publication No. 800‑77, Final). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-77> [ijisme.org+10nvlpubs.nist.gov+10nvlpubs.nist.gov+10](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-77.pdf?utm_source=chatgpt.com)

McKay, K. A., & Cooper, D. A. (2019, August 29). *Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations* (NIST SP 800‑52r2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-52r2>

*For additional information on APA Style formatting, please consult the* [*APA Style Manual, 7th*](https://apastyle.apa.org/style-grammar-guidelines) *Edition.*