

1.A.8 Essay – HTTP vs HTTPS

HTTP (occupying port 80) and HTTPS (occupying port 443) are quite similar in protocol, however HTTPS involves the exchanging of keys with a TLS/SSL certificate which contains encryption keys for securing a connection's data through obfuscation. This means while HTTP data can be captured with Wireshark or tShark in plain-text, the same cannot be said for HTTPS.

Changing from HTTP to HTTPS affects our real-life by providing more secure website interactions that cannot be easily sniffed. This encryption is especially important on eCommerce, banking, and social networking websites. In order to decrypt the packets captured in Wireshark or tShark (if using terminal or command prompt), the private key of the website must be known. This means that HTTPS isn't 100% secure as the private key can be obtained but, it provides another hoop for one to go through in order to capture user's personal or financial information. The chances for someone to have the private key of an important website being used by the user whose packets are being captured are slim.

The SSL transaction uses a widely distributed public key (to clients of the server) and a tightly held private key (on the server side) for decrypting the messages encrypting using the public key. "Anyone with access to the public key (i.e. the certificate) can verify that the digital signature is authentic without having to know the secret private key" (SSL.com, 2015). At its core the private key is "a text file used initially to generate a Certificate Signing Request (CSR), and later to secure and verify connections using the certificate created per that request" (SSL.com, 2015).

If the improved security wasn't enough of a push towards adopting HTTPS, as of December 2015, Google started prioritizing HTTPS websites in its search results (Google, 2015). This means even purely informational HTTP sites that don't benefit as much as others adopting HTTPS are strongly encouraged to do so.

References

- SSL.com. (2015, April 7). FAQ – What Is a Private Key? Retrieved from <https://info.ssl.com/faq-what-is-a-private-key/>
- Google. (2015, December 17). Indexing HTTPS pages by default. Retrieved from <https://webmasters.googleblog.com/2015/12/indexing-https-pages-by-default.html>
- Lakhera, P. (2017, March 23). HTTP/HTTPS Analysis Using Wireshark. Retrieved from <https://medium.com/devops-world/http-https-analysis-using-wireshark-cbe07c23520>