The cryptographic protocols TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are used to protect network communication. While TLS is its successor and is utilized in contemporary secure connections, especially TLS 1.2 and 1.3, SSL is the older protocol; all public versions of SSL are now deprecated and vulnerable .

Data integrity, server authentication, and encryption are all provided by HTTPS, which is HTTP layered over SSL/TLS. This means that data in transit is difficult to read or alter. On the other hand, HTTP only transmits data in plain text, which leaves it open to data injection, man-in-the-middle (MITM) attacks, and eavesdropping.

When SSL/TLS is not used or is configured incorrectly, web applications are vulnerable to a number of threats, including the theft of user credentials, cookies, or personal information; spoofing by attackers to pose as servers; traffic interception or modification; noncompliance with legal or regulatory requirements; and a decline in reputation, trust, or search engine rankings. Vulnerabilities can also result from weak cypher suites, expired certificates, or support for insecure protocols.

Instances of SSL/TLS that is missing, expired, or incorrectly configured causing harm have occurred in the real world. For instance, during its hack, Equifax's breach resulted in the expiration of more than 300 certificates, including a crucial monitoring certificate.

Reference list

Amazon Web Services (n.d.). *SSL vs TLS - Comparing Communication Protocols - AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/compare/the-difference-between-ssl-and-tls/.

Cloudflare (2024). How Does SSL Work? | SSL Certificates and TLS | Cloudflare. *Cloudflare*. [online] Available at: https://www.cloudflare.com/learning/ssl/how-does-ssl-work/.

Postal, C. (2024). *What is the SSL Not Available Risk?* | *UpGuard*. [online] Upguard.com. Available at: https://www.upguard.com/blog/what-is-the-ssl-not-available-risk.

Wikipedia. (2022). *DROWN attack*. [online] Available at: https://en.wikipedia.org/wiki/DROWN_attack.