SL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptography's network communication protocols. TLS superseded, and also replaced, SSL as the latter, more secure version, and TLS 1.2 and 1.3 today continue to keep abreast of modern standards (Cloudflare, no date; Gigamon, 2019). HTTPS (Hypertext Transfer Protocol over SSL/TLS) encloses HTTP over SSL/TLS, securing data in transit between clients and servers, whereas HTTP transmits data in plaintext, subject to intercept and alteration (DreamHost, 2020).

The risks of not using SSL/TLS include exposing sensitive user information (passwords and credit card numbers) to eavesdropping, aiding in man-in-the-middle attacks, and losing user trust as browsers label sites as "not secure" (Gigamon, 2019). Actual attacks include 2013's shutdown of software firm Code Spaces, whereby attackers exploited poor SSL practice to gain control over their AWS account, quickly resulting in the company closing down; another example is 2014's Heartbleed vulnerability, an abrupt defect in the OpenSSL library exposing private keys and sensitive information to millions of sites (DreamHost, 2020).

Bibliograghy  
Cloudflare (no date) *SSL*. Available at: <https://developers.cloudflare.com/ssl/> (Accessed: 22 September 2025).

Gigamon (2019) *Gigamon’s guide to communications security: What is SSL, TLS, and HTTPS?* 6 September. Available at: <https://blog.gigamon.com/2019/09/06/gigamons-guide-to-communications-security-what-is-ssl-tls-and-https/> (Accessed: 22 September 2025).

DreamHost (2020) *The ultimate guide to SSL and TLS*. Available at: <https://www.dreamhost.com/blog/ultimate-guide-ssl-tls/> (Accessed: 22 September 2025).

Github Link: https://github.com/VCDW2025TD/ice-task-1-insy7314-2025-ST10377715.git