**ST10355439**

**INSY7314**

**Research Activity: Why SSL?**

Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications. A protocol that uses encryption to provide internet security. Transport Layer Security (TLS) is the evolved form of SSL.

Hypertext Transfer Protocol Secure is Hypertext Transfer Protocol with encryption, using SSL/TLS for all HTTP requests and responses.

SSL stops certain kinds of cyber-attacks and prevents attackers from tampering with data in transit.

A website not using SSL will be vulnerable to cyber-attacks such as man-in-the-middle attacks.

The freak vulnerability (discovered in 2015) is a downgrade attack where the threat actor forces SSL/TLS connections to use weak cypher suites with 40- and 56-bit cryptographic keys.