SENG2250/6250 System and Network Security
Self-Quiz Week 9, Semester 2, 2020

True/False Questions

1. OSI security architecture describes seven layers, including physical, data-link, network, transport, session, presentation, and application layers.
   False. OSI security architecture offers a systematic way of defining security requirements (e.g., authentication, access control) and characterizing the approaches (e.g., encryption, digital signature) to achieve these requirements. OSI security architecture considered security services, mechanisms, and attacks.

2. Non-repudiation only considers the integrity/origin of a message.
   False, non-repudiation can also provide proof of the delivery of messages, i.e., the receiver cannot deny having received the messages.

3. Secure Socket Layer (SSL) works on the presentation layer of the OSI model.
   False. SSL does not fit in a single layer of the OSI model nor the TCP/IP model. It uses across multiple layers, such as the presentation and transport layers of the OSI model.

4. Alert protocol is used to convey SSL-related alert to the peer entity that the alert message is compressed and encrypted.
   True.

5. A public key certificate is mandatory for performing SSL handshake protocol.
   False. A public key certificate is optional for both client and server. Note that if none certificate is used for SSL handshake, the handshake will not be secure against the man-in-the-middle attacks when Diffie-Hellman key exchange is used.

Short-Answer Questions

6. What is the difference(s) between the SSL connection and SSL session?
   - SSL Connection
     - *Peer-to-peer relationship, transient.*
     - *Every connection is associated with one session.*
   - SSL Session
     - *An association between a server and a client.*
     - *Created by the handshake protocols.*
     - *Defines a set of cryptographic security parameters.*
     - *A session could be shared by multiple connections.*