SENG2250/6250 System and Network Security
Self-Quiz Week 8, Semester 2, 2020

True/False Questions.

1. Simple Object Access Protocol (SOAP) defines semantics for machine-to-machine communication over the networked (distributed) system.
   False. SOAP defines a framework for message exchange, but it does not specify application semantics.

2. WSS provides confidentiality and integrity for securing SOAP that WSS applies specific security mechanisms, such as AES and Kerberos, to achieve the objectives.
   False. WSS is flexible and is designed to be used as the basis for the construction of a wide variety of security models, including PKI, Kerberos, and SSL. However, it does not force to use a specific mechanism.

3. SAML protocol can provide authentication and authorisation services.
   True.

4. SAML assertion is an essential unit of SAML, so it originally provides security services, such as confidentiality, integrity, and authenticity.
   False. SMAL assertion defines the framework to convey claim, statement, and declaration. However, it does not provide confidentiality and integrity. We could use XML signature/encryption for security protection or use SSL/TLS connection.

5. OAuth is an authorisation standard rather than an authentication standard.
   True.

Short-Answer Questions

6. In OAuth protocol, the authorization server provides an authorization code to the client, but not an access token. Then, the client has to exchange an access token by using the authorization code.
   In step 3, the authorization code is delivered to the client via the user-agent. There is a significant security risk if the user-agent can capture the access token. For example, malware (or compromised user-agent) can use the captured token to access the resource directly. Also, the server needs to do further checks, in step 4, and confirm if the client is honest.