SENG2250/6250 System and Network Security
Self-Quiz Week 11, Semester 2, 2020

True/False Questions

1. Hiding the detail of the cryptographic algorithm is an effective way to avoid its potential threats being exposed.
   False. Hiding the algorithm does not solve the issues. It is vulnerable to reverse-engineering.

2. IEEE 802.11 refers to a family of specifications for Wireless LAN (WLAN).
   True.

3. WEP defines data encryption and integrity checking that can provide message confidentiality and integrity.
   False. WEP uses RC4-based, 40-bit key encryption to prevent an intruder from accessing the message. However, the key size is too short to achieve sufficient security. WEP integrity checking uses CRC-32, which is a non-cryptographic checksum. An adversary can modify a message without being detected by CRC-32.

4. Extensible authentication protocol (EAP) defines an authentication framework that supports multiple authentication methods, such as TLS and MD5.
   True.

5. TKIP fixes the problems with WEP by using a new encryption algorithm and cryptographic hash function.
   False. TKIP uses a longer secret key while the underlying encryption algorithm is still the RC4.

Short-Answer Questions

6. Briefly explain the three essential components of IEEE 802.1X.
   Supplicant – Wireless terminal, basically the user or client.
   Authenticator – Access point, responsible for communication with Supplicant, submits information received from Supplicant to Authentication Server, which can then check Supplicant credentials for correct authorization.
   Authentication Server – Provides authentication services to Authenticator to determine whether Supplicant is authorized to access services provided by the Authenticator.