SENG2250/6250 System and Network Security
Self-Quiz Week 10, Semester 2, 2020

True/False Questions

1. IPSec is a suite of standards for providing a rich set of security services at the network layer.
   True.

2. IPSec transport mode can hide the source and destination IP addresses.
   False. IPSec transport mode cannot hide the IP addresses. Instead, the tunnel mode can protect the actual source and destination IPs.

3. The authentication header (AH) protocol provides the integrity checking value (ICV) for all the IP header fields.
   False. ICV can only authenticate the immutable or mutable but predictable fields.

4. IPSec uses a policy-based approach to implement access control services.
   True.

5. In the Internet key exchange (IKE) phase 1, if the aggressive mode is used, then phase 2 can be removed for faster key exchange (i.e. handshake).
   False. IKE must run in two phases. In phase 1, the aggressive mode runs faster than the main mode, but the aggressive mode does not provide identity protection. The output of phase 1 is IKE SA, no matter which mode is used. Then, the IKE SA will be used in phase 2 (for security protection) and the phase 2 outputs an ESP or AH SA.

Short-Answer Questions

6. What is the purpose of using cookies in IKE?
   Cookies are used to avoid denial of service attacks, which exploit the computational expense of calculating keys. The idea is to force legitimate parties to carry out a cookie exchange before significant computations are carried out.