**Chapter 24 – Wireless Network Security**

**TRUE/FALSE QUESTIONS:**

T F 1. The concerns for wireless security, in terms of threats, and

countermeasures, are different to those found in a wired environment, such as an Ethernet LAN or a wired wide-area network.

T F 2. The most significant source of risk in wireless networks in the

underlying communications medium.

T F 3. The wireless access point provides a connection to the network or

service.

T F 4. The transmission medium carries the radio waves for data transfer.

T F 5. Company wireless LANs or wireless access points to wired LANs in

close proximity may create overlapping transmission ranges.

T F 6. An extended service set (ESS) is a set of stations controlled by a

single coordination function.

T F 7. Any device that contains an IEEE 802.11 conformant MAC and

physical layer is a basic service set.

T F 8. WPA2 incorporates all of the features of the IEEE 802.11i WLAN

security specifications.

T F 9. The MAC service data unit contains any protocol control

information needed for the functioning of the MAC protocol.

T F 10. CRC is an error detecting code.

T F 11. In most data-link control protocols, the data-link protocol entity is

responsible not only for detecting errors using the CRC, but for

recovering from those errors by retransmitting damaged frames.

T F 12. The association service enables transfer of data between a station

on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN.

T F 13. The primary purpose of the MAC layer is to transfer MSDUs

between MAC entities.

T F 14. The purpose of the discovery phase is for an STA and an AP to

recognize each other, agree on a set of security capabilities, and establish an association for future communication using those security capabilities.

T F 15. The purpose of the authentication phase is to maintain backward

compatibility with the IEEE 802.11 state machine.

**MULTIPLE CHOICE QUESTIONS:**

1. A wireless client can be \_\_\_\_\_\_\_.

A. a cell phone B. a Wi-Fi enabled laptop

C. a Bluetooth device D. all of the above

2. A wireless access point is a \_\_\_\_\_\_\_.

A. cell tower B. Wi-Fi hot spot

C. wireless access point to a LAN or WAN D. all of the above

3. The wireless environment lends itself to a \_\_\_\_\_\_ attack because it is so easy for the attacker to direct multiple wireless messages at the target.

A. DoS B. man-in-the-middle

C. network injection D. identity theft

4. An example of a(n) \_\_\_\_\_\_\_\_\_\_ attack is one in which bogus reconfiguration commands are used to affect routers and switches to degrade network performance.

A. identity theft B. ad hoc network

C. network injection D. man-in-the-middle

5. A(n) \_\_\_\_\_\_\_\_\_\_ is any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.

A. ESS B. access point

C. distribution system D. MPDU

6. The unit of data exchanged between two peer MAC entities using the services of the physical layer is a(n) \_\_\_\_\_\_\_\_\_\_\_\_.

A. extended service set B. MPDU

C. MSDU D. station

7. A system used to interconnect a set of basic service sets and LANs to create an extended service set is a \_\_\_\_\_\_\_\_\_.

A. distribution system B. coordination function

C. MAC data unit D. wireless access system

8. The function of the \_\_\_\_\_\_\_\_ layer is to control access to the transmission medium and to provide an orderly and efficient use of that capacity.

A. CRC B. MPDU

C. MAC D. MSDU

9. The final form of the 802.11i standard is referred to as \_\_\_\_\_\_\_\_.

A. WEP B. RSN

C. Wi-Fi D. WPA

10. In order to accelerate the introduction of strong security into WLANs the Wi-Fi Alliance promulgated \_\_\_\_\_\_\_\_, a set of security mechanisms that eliminates most 802.11 security issues, as a Wi-Fi standard.

A. WPA B. WEP

C. RSN D. MAC

11. The specification of a protocol, along with the chosen key length, is known as a \_\_\_.

A. distribution set B. open system

C. cipher suite D. realm

12. A \_\_\_\_\_\_\_\_ is a secret key shared by the AP and a STA and installed in some fashion outside the scope of IEEE 802.11i.

A, pre-shared key B. master session key

C. pairwise master key D. group master key

13. The MPDU exchange for distributing pairwise keys is known as the \_\_\_\_\_\_\_.

A. pseudorandom function B. cryptographic function

C. nonce D. 4-way handshake

14. \_\_\_\_\_\_ is the recommended technique for wireless network security.

A. Using encryption

B. Using anti-virus and anti-spyware software

C. Turning off identifier broadcasting

D. All of the above

15. The smallest building block of a wireless LAN is a \_\_\_\_\_\_.

A. BSS B. ESS

C. WPA D. CCMP

**SHORT ANSWER QUESTIONS:**

1. The security requirements are: confidentiality, integrity, availability, authenticity, and \_\_\_\_\_\_\_\_\_\_.
2. The wireless environment consists of three components that provide point of attack: the wireless client, the transmission medium, and the \_\_\_\_\_\_\_\_\_.
3. A \_\_\_\_\_\_\_\_\_\_\_\_ attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device.
4. A \_\_\_\_\_\_\_\_\_\_ attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources.
5. A \_\_\_\_\_\_\_\_\_\_ attack targets wireless access points that are exposed to non-filtered network traffic, such as routing protocol messages or network management messages.
6. The principal threats to wireless transmission are disruption, \_\_\_\_\_\_\_\_\_\_\_\_\_, and altering or inserting messages.
7. Like TKIP, CCMP provides two services: message integrity and \_\_\_\_\_\_\_\_.
8. Two types of countermeasures are appropriate to deal with eavesdropping: signal-hiding techniques and \_\_\_\_\_\_\_\_\_\_\_\_.
9. The lowest layer of the IEEE 802 reference model is the \_\_\_\_\_\_\_\_\_\_ layer.
10. The fields preceding the MSDU field are referred to as the \_\_\_\_\_\_\_\_\_.
11. The field following the MSDU field is referred to as the \_\_\_\_\_\_\_\_\_\_\_.
12. The two services involved with the distribution of messages within a DS are distribution and \_\_\_\_\_\_\_\_\_.
13. The 802.11i RSN security specification defines the following services: authentication, privacy with message integrity, and \_\_\_\_\_\_\_\_.
14. There are two types of keys: \_\_\_\_\_\_\_\_ used for communication between a STA and an AP and group keys used for multicast communication.
15. At the top level of the group key hierarchy is the \_\_\_\_\_\_\_\_\_\_\_.