**Chapter 18:** **Wireless Network Security**

**TRUE OR FALSE**

T F 1. IEEE 802.11 is a standard for wireless LANs.

T F 2. Wireless networks, and the wireless devices that use them,

introduce a host of security problems over and above those found

in wired networks.

T F 3. Sensors and robots, are not vulnerable to physical attacks.

T F 4. The integration 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 5. MAC spoofing occurs when an attacker is able to eavesdrop on

network traffic and identify the MAC address of a computer with

network privileges.

T F 6. The DS can be a switch, a wired network, or a wireless network.

T F 7. The pairwise master key is derived from the group key.

T F 8. IEEE 802.11 defines seven services that need to be provided by the

wireless LAN to achieve functionality equivalent to that which is

inherent to wired LANs.

T F 9. Handheld PDAs pose a security risk in terms of both eavesdropping

and spoofing.

T F 10. The actual method of key generation depends on the details of the

authentication protocol used.

T F 11. The use of 802.1X cannot prevent rogue access points and other

unauthorized devices from becoming insecure backdoors.

T F 12. The principal threats to wireless transmission are eavesdropping,

altering or inserting messages, and disruption.

T F 13. The use of encryption and authentication protocols is the

standard method of countering attempts to alter or insert

transmissions.

T F 14. You should allow only specific computers to access your wireless

network.

T F 15. Security policies for mobile devices should assume that any

mobile device will not be stolen or accessed by a malicious party.

**MULTIPLE CHOICE**

1. The term used for certified 802.11b products is \_\_\_\_\_\_\_\_\_\_\_ .

A. WAP B. Wi-Fi

C.WEP D. WPA

1. The layer of the IEEE 802 reference model that includes such functions as encoding/decoding of signals and bit transmission/reception is the \_\_\_\_\_\_\_\_\_ .

A. physical layer B. control layer

C. logical link layer D. media access layer

1. In a(n) \_\_\_\_\_\_\_\_\_\_ situation, a wireless device is configured to appear

to be a legitimate access point, enabling the operator to steal passwords

from legitimate users and then penetrate a wired network through a legitimate wireless access point.

A. malicious association B. identiy theft

C. network injection D. ad hoc network

1. \_\_\_\_\_\_\_\_\_\_\_ and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.

A. DoS B. Accidental association

C. Nontraditional networks D. Ad hoc networks

1. The function of the \_\_\_\_\_\_\_\_\_\_ is to on transmission assemble data into a frame, on reception disassemble frame and perform address recognition and error detection, and govern access to the LAN transmission medium.

A. transmission layer B. logical layer

C. media access control layer D. physical layer

1. The master session key is also known as the \_\_\_\_\_\_\_\_\_\_ key.

A. AAA B. GTK

C. MIC D. STA

1. The \_\_\_\_\_\_\_\_\_\_ is the information that is delivered as a unit between MAC users.

A. MSDU B. DS

C. MPDU D. BSS

1. The \_\_\_\_\_\_\_\_\_\_ layer keeps track of which frames have been successfully received and retransmits unsuccessful frames.

A. transmission B. media access control

C. logical link control D. physical layer

1. The purpose of the discovery phase in the \_\_\_\_\_\_\_\_\_\_\_ is for a 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.

A. WPA B. RSN

C. TKIP D. WAE

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

A. extended service B. distribution system

C. cipher suite D. RSN

1. The \_\_\_\_\_\_\_\_\_ is used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.

A. MIC key B. EAPOL-KEK

C. EAPOL-KCK D. TK

1. The PMK is used to generate the \_\_\_\_\_\_\_\_\_ which consists of three keys to be used for communication between a STA and AP after they have been mutually authenticated.

A. AAA Key B. GTK

C. PTK D. PSK

1. A \_\_\_\_\_\_\_\_\_\_ is any device that contains an IEEE 802.11 conformant MAC and physical layer.

A. station B. MPU

C. service data unit D. MSDU

1. The first 802.11 standard to gain broad industry acceptance was \_\_\_\_\_\_\_\_\_.

A. 802.11i B. 802.11a

C. 802.11g D. 802.11b

1. \_\_\_\_\_\_\_\_\_\_\_\_ can occur when a company’s wireless LAN or wireless access points to wired LANs in close proximity and may create overlapping transmission ranges. A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.

A. Network injection B. Denial of service attacks

C. Man-in-the-middle attacks D. Accidental association

**SHORT ANSWER**

1. In simple terms, the wireless environment consists of three components that

provide point of attack: the endpoint, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_, and the access point.

1. 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.
2. \_\_\_\_\_\_\_\_\_\_ is the primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS.
3. To certify interoperability for 802.11b products an industry consortium named the \_\_\_\_\_\_\_\_\_\_ was formed.
4. The \_\_\_\_\_\_\_\_\_\_ function is the logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
5. Derived from the GMK, the \_\_\_\_\_\_\_\_\_ is used to provide confidentiality and integrity protection for multicast/broadcast user traffic.
6. An \_\_\_\_\_\_\_\_\_\_ is a set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
7. The \_\_\_\_\_\_\_\_\_\_ layer is responsible for detecting errors and discarding any frames that contain errors.
8. The smallest building block of a wireless LAN is a \_\_\_\_\_\_\_\_\_\_ which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.
9. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated \_\_\_\_\_\_\_\_\_\_ as a set of security mechanisms for the Wi-Fi standard.
10. The MPDU authentication phase consists of three phases. They are: connect to AS, EAP exchange and \_\_\_\_\_\_\_\_\_ .
11. Forming a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time, \_\_\_\_\_\_\_\_\_\_ are used for communication between a pair of devices typically between a STA and an AP.
12. The MPDU exchange for distributing pairwise keys is known as the \_\_\_\_\_\_\_\_\_ which the STA and SP use to confirm the existence of the PMK, to verify the selection of the cipher suite, and to derive a fresh PTK for data sessions.
13. The main threat involving wireless access points is unauthorized access to the network. The principal approach for preventing success is the \_\_\_\_\_\_\_\_\_\_ standard for port-based network access control.
14. The IEEE 802.11 protocol stack consists of the logical link control layer, the medium access control layer, and the \_\_\_\_\_\_\_\_\_ layer.