**TRUE/FALSE**

1. Wireless access control through MAC address filtering is the same as access restrictions.

   ANS: F PTS: 1 REF: 40

2. WEP relies on a secret key shared between a wireless client device and the access point.

   ANS: T PTS: 1 REF: 43

3. When WEP is used for shared key authentication it is serving a dual function of encryption and authentication.

   ANS: T PTS: 1 REF: 48

4. The SSID can be easily discovered even when it is not contained in beacon frames.

   ANS: T PTS: 1 REF: 52

5. Deploying dynamic WEP is a very expensive solution that involves a lot of effort.

   ANS: F PTS: 1 REF: 59

**MULTIPLE CHOICE**

1. Access control is intended to guard the ____ of information by making it accessible only to authorized users.
   a. confidentiality
   b. availability
   c. integrity
   d. non-repudiation

   ANS: B PTS: 1 REF: 38

2. Wired equivalent privacy (WEP) is intended to guard one of the three CIA characteristics of information, namely ____.
   a. confidentiality
   b. integrity
   c. availability
   d. non-repudiation

   ANS: A PTS: 1 REF: 41

3. Changing the original text to a secret message using cryptography is known as ____.
   a. ciphertext
   b. decryption
   c. encryption
   d. plaintext

   ANS: C PTS: 1 REF: 42

4. In ____, a shared secret key is used to encrypt the cleartext as well as decrypt the ciphertext.
   a. public key cryptography
   b. asymmetric encryption
   c. asymmetric cryptography
   d. private key cryptography

   ANS: D PTS: 1 REF: 43

5. In WEP, the ____ is a cyclic redundancy check (CRC) value calculated with a checksum based on the contents of the text.
   a. initialization vector (IV)
   b. pseudo-random number generator (PRNG)
   c. integrity check value (ICV)
   d. RC4

   ANS: C PTS: 1 REF: 45

6. In WEP, the ____ is a 24-bit value that changes each time a packet is encrypted.
   a. initialization vector (IV)
   b. pseudo-random number generator (PRNG)
   c. integrity check value (ICV)
   d. RC4

   ANS: A PTS: 1 REF: 45

7. A stream cipher takes one character and replaces it with another character. This output is known as the ____.
   a. initialization vector
   b. integrity check value
   c. cyclic redundancy check
   d. keystream

   ANS: D PTS: 1 REF: 45

8. ____ requires the *wireless device* (and not the user) to be authenticated prior to being connected to the network.
   a. SSID
   b. Wireless authentication
   c. Wired confidentiality
   d. Wireless availability

   ANS: B PTS: 1 REF: 47

9. A(n) ____ carries information about the data rates that a device can support along with the Service Set Identifier (SSID) of the network it wants to join.
   a. association request frame
   b. CRC
   c. PRNG
   d. ICV

   ANS: A PTS: 1 REF: 47

10. At regular intervals (normally every 100 ms) an AP sends a(n) ____ to announce its presence and to provide the necessary information for other devices that want to join the network.
    a. association request frame
    b. CRC
    c. ICV
    d. beacon frame

    ANS: D PTS: 1 REF: 49

11. With ____ scanning a wireless device simply listens for a beacon frame for a set period of time.
    a. active
    b. passive
    c. interactive
    d. moving

    ANS: B PTS: 1 REF: 49

12. The APs can be positioned so that the cells overlap to facilitate movement between cells, known as ____.
    a. SSID broadcast
    b. handoff
    c. roaming
    d. scanning

ANS: C PTS: 1 REF: 51

13. In a ____ attack, an attacker attempts to create every possible key combination by using a program to systematically change one character at a time.
    a. social engineering
    b. brute force
    c. dictionary
    d. birthday

    ANS: B PTS: 1 REF: 53

14. A ____ attack takes each word from a dictionary and encodes it in the same way the passphrase was encoded.
    a. social engineering
    b. brute force
    c. dictionary
    d. birthday

    ANS: C PTS: 1 REF: 53

15. To encrypt packets WEP can use only a 64-bit or ____-bit number.
    a. 72
    b. 90
    c. 110
    d. 128

    ANS: D PTS: 1 REF: 55

16. Because of the weaknesses of the implementation of WEP it is possible for an attacker to identify two packets derived from the same IV (called a(n) ____).
    a. collision
    b. keystream
    c. ICV
    d. CRC vector

    ANS: A PTS: 1 REF: 56

17. WEP2 uses a different authentication system known as ____.
    a. RADIUS
    b. MS-CHAPS
    c. LDAP
    d. Kerberos

    ANS: D PTS: 1 REF: 59

18. ____ was developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of network users.
    a. Kerberos
    b. Dynamic WEP
    c. WEP2
    d. LDAP

    ANS: A PTS: 1 REF: 59

19. ____ solves the weak initialization vector (IV) WEP problem by rotating the keys frequently.
    a. WEP2
    b. Dynamic WEP
    c. SSID
    d. Roaming

    ANS: B PTS: 1 REF: 59

20. ____ traffic is traffic destined for only one address.
    a. Severalcast
    b. Multicast
    c. Unicast
    d. Broadcast

    ANS: C PTS: 1 REF: 59

21. ____ traffic is traffic sent to all users on the network.
    a. Unicast
    c. Singlecast

b. Broadcast
d. Multicast

ANS: B PTS: 1 REF: 59

**COMPLETION**

1. A(n) _____ acts as the central base station for the wireless network.

   ANS:
   access point (AP)
   access point
   AP

   PTS: 1 REF: 39

2. _____ is the science of transforming information so that it is secure while it is being transmitted or stored.

   ANS: Cryptography

   PTS: 1 REF: 42

3. The IEEE standard specifies that the access points and devices can hold up to four shared secret keys, one of which must be designated as the _____.

   ANS: default key

   PTS: 1 REF: 44

4. A wireless device is set to look for beacon frames from the AP. This is known as _____.

   ANS: scanning

   PTS: 1 REF: 49

5. In WEP, RC4 uses a(n) _____ to create the keystream.

   ANS:
   pseudo random number generator (PRNG)
   pseudo random number generator
   PRNG

   PTS: 1 REF: 57

**MATCHING**

*Match each item with an statement below:*

a. Access control
b. Access restrictions
c. Cipher
d. RC4
e. SSID
f. Keystream attack
g. AirSnort
h. WEP2
i. Shoulder surfing

1. the “network name” for the wireless network.
2. stream cipher that accepts keys up to 128 bits in length.
3. an encryption algorithm.
4. tool to perform WEP attacks.
5. can limit a user’s access to the Internet.
6. looking over someone’s shoulder.
7. adds two new security enhancements to WEP.
8. method of determining the keystream by analyzing two packets that were created from the same IV.
9. method of restricting access to resources.

| | | | | | |
|---|---|---|---|---|---|
| 1. | ANS: E | PTS: 1 | | REF: 47 | |
| 2. | ANS: D | PTS: 1 | | REF: 45 | |
| 3. | ANS: C | PTS: 1 | | REF: 42 | |
| 4. | ANS: G | PTS: 1 | | REF: 58 | |
| 5. | ANS: B | PTS: 1 | | REF: 40 | |
| 6. | ANS: I | PTS: 1 | | REF: 53 | |
| 7. | ANS: H | PTS: 1 | | REF: 59 | |
| 8. | ANS: F | PTS: 1 | | REF: 56 | |
| 9. | ANS: A | PTS: 1 | | REF: 38 | |

**SHORT ANSWER**

1. What is a MAC address?

   ANS:
   The MAC address is a hardware address that uniquely identifies each node of a network. Other names for the MAC address are vendor address, vendor ID, NIC address, Ethernet address, and physical address.

   The MAC address is a unique 48-bit number that is “burned” into the network interface adapter when it is manufactured. This number consists of two parts: a 24-bit organizationally unique identifier (OUI), sometimes called a “company ID,” which references the company that produced the adapter, and a 24-bit individual address block (IAB), which uniquely identifies the card itself.

   PTS: 1 REF: 39

2. What was the criteria used by the IEEE 802.11 committee to design WEP?

   ANS:
   The IEEE 802.11 committee designed WEP to meet the following criteria:
   * *Efficient*—The WEP algorithm must be proficient enough to be implemented in either hardware or software.
   * *Exportable*—WEP must meet the guidelines set by the U.S. Department of Commerce so that the wireless device using WEP can be exported overseas.
   * *Optional*—The implementation of WEP in wireless LANs is an optional feature.
   * *Reasonably strong*—The security of the algorithm lies in the difficulty of determining the secret keys through attacks. This in turn is related to the length of the secret key and the frequency of changing keys. WEP was to be “reasonably” strong in resisting attacks.
   * *Self-synchronizing*—When using WEP, each packet must be separately encrypted. This is to prevent a single lost packet from making subsequent packets indecipherable.

PTS: 1 REF: 43

3. What are the options for creating keys in WEP?

   ANS:
   IEEE 802.11WEP shared secret keys must be a minimum of 64 bits in length. Most vendors add an option to use a larger 128-bit shared secret key for added security (a longer key is more difficult to break).Keys are created by the user entering the same string of either ASCII or hexadecimal characters on both the device and the AP. The options for creating keys are:
   * 64-bit key—Created by entering 5 ASCII characters (for example *5y7js*) or 10 hexadecimal characters (for example 0x*456789ABCD*) (the 0x preceding the characters indicate it is a hexadecimal number).
   * 128-bit key—Created by entering 13 ASCII characters (for example *98jui2wss35u4*) or 26 hexadecimal characters (for example 0x*33445566778899OOAABBCCDDEE*).
   * Passphrase—Created by entering a specific number of ASCII characters (for example *christmasholiday*), which then generates a hexadecimal key.

   PTS: 1 REF: 43

4. Describe the main characteristics of the open system authentication method.

   ANS:
   There are two types of authentication supported by the 802.11 standard. Open system authentication is the default method. A device discovers a wireless network in the vicinity through scanning the radio frequency and sends a frame known as an association request frame to the AP. The frame carries information about the data rates that the device can support along with the Service Set Identifier (SSID) of the network it wants to join. The SSID serves as the “network name” for the wireless network and can be any alphanumeric string from 2 to 32 characters. After receiving the association request frame, the access point compares the SSID received with the actual SSID of the network. If the two match then the wireless device is authenticated.

   PTS: 1 REF: 47

5. Describe the main characteristics of the shared key authentication method.

   ANS:
   Shared key authentication is an authentication method in which the WEP default key is used. A wireless device sends a frame to the AP and the AP sends back a frame that contains a block of text known as the challenge text. The wireless device must encrypt the text with the default key and return it to the AP. The AP will then decrypt what was returned to see if it matches the original challenge text. If it does, the device is authenticated and allowed to become part of the network (known as association). Shared key authentication is based upon the fact that only pre-approved wireless devices are given the shared key.

   PTS: 1 REF: 47-48

6. Briefly explain how turning off the beaconing of the SSID affects roaming in a wireless network environment.

   ANS:

Turning off SSID beaconing prevents wireless devices from freely roaming from one wireless network to another. To increase the area of coverage of a wireless LAN, multiple access points are installed with areas of overlap, much like cells in a cellular telephone system. The APs can be positioned so that the cells overlap to facilitate movement between cells, known as roaming. When a mobile wireless user (perhaps carrying a wireless laptop computer) enters into the range of more than one AP, the wireless device will choose an AP based on signal strength (some also look at packet error rates). Mobile devices constantly survey the radio frequencies at regular intervals to determine if a different AP can provide better service. If it finds one (perhaps because the user has moved closer to it), then the device automatically attempts to associate with the new AP (this process is called a handoff).

PTS: 1 REF: 51

7. Briefly explain how WEP implementation violates the cardinal rule of cryptography: anything that creates a detectable pattern must be avoided.

ANS:
WEP implementation violates the cardinal rule of cryptography: anything that creates a detectable pattern must be avoided. This is because patterns provide an attacker with valuable information to break the encryption. The implementation of WEP creates a detectable pattern for attackers. IVs are 24-bit numbers, meaning there are 16,777,216 possible values. An AP transmitting at only 11 Mbps can send and receive 700 packets each second. If a different IV were used for each packet, then the IVs would start repeating in fewer than seven hours (a “busy” AP can produce duplicates in fewer than five hours). An attacker who captures packets for this length of time can see the duplication and use it to crack the code.

Yet it does not always require seven hours of capturing packets to see the IV repeat. Some wireless systems always start with the same IV after the system is restarted and then follow the same sequence of incrementing IVs.

PTS: 1 REF: 55-56

8. What are some of the tools used to perform WEP attacks?

ANS:
WEP attacks can be performed through any one of a number of tools that are freely available on the Internet. Some of the best known include AirSnort, Aircrack, ChopChop WEP Cracker, and WEP Crack. However, these tools require a certain degree of computer experience to use. Only certain wireless NIC adapter cards with specific drivers can be used, and almost all of these tools were developed under the Linux operating system and are designed to function under Linux. Although a few of these tools have been ported to the Windows operating system, they require special supporting software packages to properly function. Also, the length of time needed to capture enough packets to break WEP can be several (5 to 7) hours, depending on the volume of traffic.

PTS: 1 REF: 58

9. What are the main characteristics of Kerberos?

ANS:

Kerberos is typically used when someone on a network attempts to use a network service, and the service wants assurance that the user is an authorized user. The user is provided a ticket that is issued by the Kerberos server, much as a driver's license is issued by the Division of Motor Vehicles. This ticket contains information linking it to the user. The user presents this ticket to the network for a service. The service then examines the ticket to verify the identity of the user. If all checks out, the user is accepted.Kerberos tickets share some of the same characteristics as a driver's license: tickets are difficult to copy (because they are encrypted), they contain specific user information, they restrict what a user can do, and they expire after a few hours or a day.

PTS: 1 REF: 59

10. What are the differences between Dynamic WEP unicast and broadcast keys?

ANS:
Dynamic WEP uses different keys for unicast traffic (traffic destined for only one address) and broadcast traffic (traffic sent to all users on the network). The unicast WEP key, which is unique to each user's session, is dynamically generated and changed frequently. This key is also changed every time the user roams to a new AP or logs out and logs back in. A separate key is used for broadcast traffic. The broadcast WEP key must be the same for all users on a particular subnet and AP because users connecting to the same AP must see the same broadcast information. Keys can be set to change frequently, such as every 15 to 30 minutes.

PTS: 1 REF: 59