Wireless Security

Learning Objective

After studying this chapter, you should be able to:

- Understand the essential elements of the IEEE 802.11 wireless LAN standard.
- Study the additional security issues arising in Wireless LANs.
- Present an overview of wireless network security approaches (WEB, WPA, WPA2), their strength and limitation.
- Understand countermeasures available to further reduce threats in wireless networks.

1.Introduction

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. Nowadays most, if not all, laptops and mobile phones around the world are equipped for WLAN. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware of.

2.WLAN Architecture

One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. IEEE 802.11 is a family of standards for wireless LANs, the most used home standards are:

- 802.11b: 5.5 Mbps and 11 Mbps. Maximum specified range 100 meters. Average throughput of ~4Mbps, range of 30-40m (indoor).
- 802.11g: Supports up to 54Mbps. Average throughput of ~20 Mbps, range of 30-40m (indoor).
- 802.11n (WI-FI 4): Typical 75Mbps and maximum of 300Mbps. Range of 70m (indoor).
- 802.11ac (Wi-Fi 5): Typical speeds ranging from 433 Mbps all the way up to several Gigabits per second, range of 30-40m (indoor).
- 802.11ax (Wi-Fi 6): Offers higher data rates and capacity, up to 9.6 Gbps, range of 30m (indoor).

2.1.WLAN Components

Basic components of a WLAN are access points (APs) and stations.

Access Points: Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna, in other word it is a bridge between wireless and wired networks. An AP operates within a specific frequency spectrum and uses 802.11 standard specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

Stations: Wireless station is a desktop, laptop, PDA, Mobile phone, a wireless sensor, or any device with a wireless network interface cards (NICs). Wireless client adapters connect station to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs (will be discussed in the following section). It connects stations wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client.

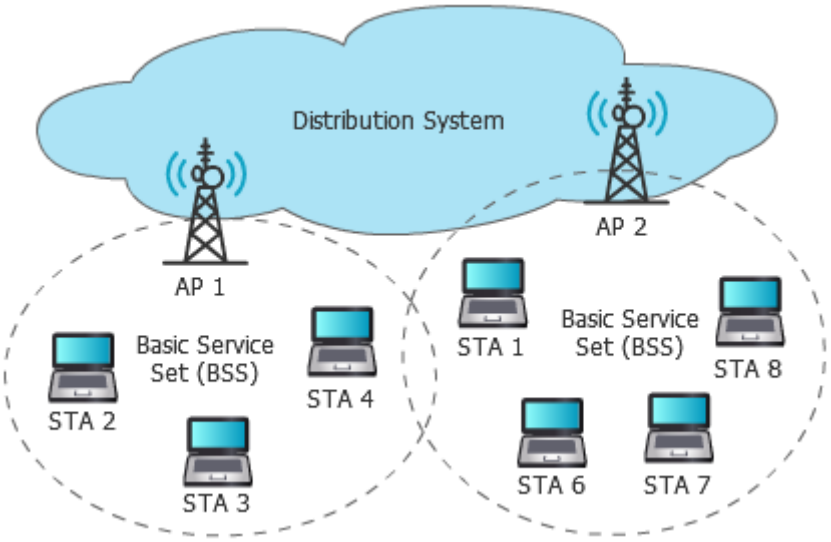
2.2.WLAN Architecture Model

The WLAN components mentioned above are connected in certain configurations. There are three main types of WLAN architecture:

Infrastructure WLAN (basic service set (BSS)): BSS WLAN consists of wireless stations and access points (AP). The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the frame is first sent from the originating station to the AP and then from the AP to the destination station. The BSS generally corresponds to what is referred to as a cell in the literature.

Independent WLAN (ad hoc LAN): The simplest WLAN configuration is an independent (or peer-to-peer) WLAN. It is a group of computers, each equipped with one wireless LAN NIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. In other word, in this mode no infrastructure is required, and the stations are self-organized. Independent networks can be set up whenever two or more wireless adapters are within range of each other.

Microcells and Roaming (extended service set (ESS)): The area of coverage for an access point is called a "microcell". The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. One of the main benefits of WLAN is user mobility. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications. Seamless roaming is only possible if the access points have a way of exchanging information as a user connection is handed off from one access point to another. In a setting with overlapping microcells, wireless nodes and access points frequently check the strength and quality of transmission. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal, in accommodating roaming from one microcell to another.



Figure(8.1): Extended Service Set

3.Security Threats for WLAN

Despite the productivity, convenience and cost advantage that WLAN offers, the 802.11 standard family faces a common set of security vulnerabilities due to the open wireless medium. We focus here on the security threats related to the wireless link between the stations and the AP, which is in many cases the last hop in the end-to-end path. We do not consider the security compromise of an AP nor the attacks on the wired network portion.

The security threats in WLAN can be roughly divided into two categories based on their scope and impact. The first category includes attacks targeting the network infrastructure:

- Channel Jamming: The attacker can jam the wireless channel in the physical layer and effectively deny network access to legitimate users, independent from whether the network is secured.
- Unauthorized Access: When authentication is not turned on, as is the case in many deployed networks, the attacker cannot only gain free network usage but also use the AP to bypass the firewall and access the internal network.
- Traffic Analysis: The attacker can analyze the overheard wireless traffic to obtain useful information, such as the network usage pattern.

The second category includes attacks against the communication between the station and the AP.

- Eavesdropping: By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because with advanced antennas, it is possible to monitor wireless traffic from a few miles away.
- Message Forgery: When the wireless link is not protected for message integrity, the attacker can inject forged messages into both directions of the communication.
- Message Replay: Even when message integrity is enforced, the attacker can replay previously recorded messages, including authentication data.
- Man-in-the-middle Attack: The attacker can manage to reside between the station and the AP, and intercept and modify the messages on-the-fly. For instance, he can set up a rogue AP or forge Address Resolution Protocol (ARP) replies that map himself to the AP's IP address. Moreover, 802.11 does not require an Access Point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's.
- Session Hijacking: The attacker can hijack an established session in two steps. He first breaks the session through wireless contention, then masquerades the legitimate station and replays the previous authentication messages.

To deal with eavesdropping in WLAN, two types of countermeasures are appropriate:

Signal-hiding Techniques: In Open System Authentication, a station must specify service set identifier (SSID) to AP when requesting association. APs can broadcast their SSID as a beacon. Organizations can take a number of measures to make it more difficult for an attacker to locate their wireless access points, including turning off (SSID) broadcasting by wireless access points, reducing signal strength to the lowest level that still provides requisite coverage, and locating wireless access points in the interior of the building, away from windows and exterior walls. Greater security

can be achieved by the use of directional antennas and of signal-shielding techniques. However, attackers can still attack APs that do not transmit SSID, by sending de-authenticate frames to client. SSID then is captured when client sends re-authenticate frames containing SSID. This technique is implemented in essid_jack tool. As a sequence, Open System Authentication only provides trivial level of security.

Encryption: Encryption of all wireless transmission is effective against eavesdropping to the extent that the encryption keys are secured. The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions.

4.Securing Wireless Transmissions

Link-layer security mechanisms can provide strong information security by encrypting and integrity-checking every message. They also reduce network security threats by preventing unauthorized access. However, they do not address the jamming and traffic analysis attacks, which require physical-layer solutions. Data communication over WLAN can also be protected at the network layer and above through end-to-end mechanisms (e.g., IPSec, VPN). However, these solutions cannot address wireless-specific attacks, such as unauthorized access or man-in-the-middle attacks. They can be used to complement link-layer mechanisms and further enhance end-to-end data security.

4.1.Wired Equivalent Privacy (WEP)

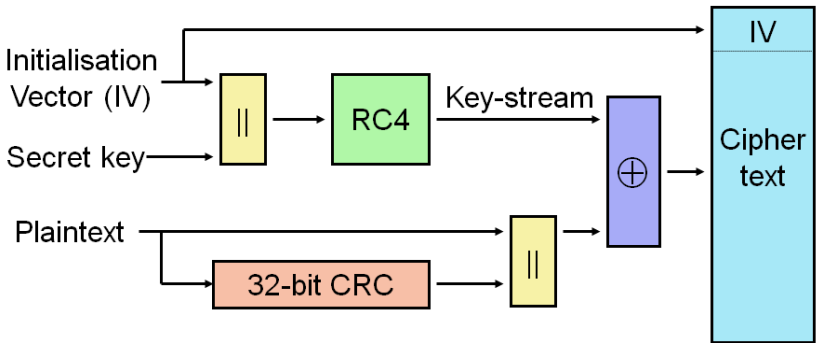
The WEP protocol was the first link-layer security mechanism introduced in 802.11 to provide a security level comparable to that with a physical wire. WEP was designed to enforce data confidentiality, data integrity, and access control through the following primitives:

- Encryption: WEP encrypts data using an RC4-based stream cipher to achieve data confidentiality.
- Integrity checksum: WEP uses cyclic redundancy check (CRC) to compute integrity checksums for the messages.

- Authentication: WEP uses a challenge–response handshake based on pre-shared keys to authenticate the stations.

The AP enforces access control by discarding all frames that are not properly encrypted. Putting these primitives together, the data transmission in WEP works in the following way figure(8.2). A secret key is shared between two communicating parties. Given a message, the sender (either the station or the AP) first computes a CRC checksum, then concatenates them into a plaintext.

The sender chooses an initialization vector (IV) and uses the RC4 algorithm to generate a keystream RC4, which is a long sequence of pseudorandom bits. The length of (IV) is 24 bits. The key length has two popular choices, 40-bit or 104-bit keys, in the so-called 64-bit and 128-bit versions respectively. The sender XORs the plaintext with the keystream into the ciphertext. Finally, the sender transmits the IV and the ciphertext.



Figure(8.2): Web Encryption

Insecurity of WEP: At first glance, WEP seems to have well addressed the security needs in WLANs by encrypting and check summing each message. However, subsequent cryptanalysis has shown otherwise, mostly due to the security flaws in the WEP design. In what follows we provide a sketch of these cryptanalysis results:

- Keystream reuse: key stream reuse means the same keystream being used to encrypt multiple messages. In such cases, the XOR-based stream cipher used in WEP can be easily broken to decrypt data traffic. Because the key is fixed, the same keystream is derived when IVs collide. Unfortunately, the fairly short length (24 bits) of IV poses a fundamental limit on the keystream space

size, regardless of the key length. The chance of keystream reuse is further increased by sharing the key among multiple stations and the AP. Whenever two entities pick the same IV, the corresponding keystream is reused.

- Linear checksum: Linear checksum can be exploited to modify messages in arbitrary ways. In addition, because the checksum is un-keyed, the attacker needs only one valid keystream to inject forged messages. This further defeats the authentication mechanism, because the attacker can now successfully complete the challenge–response handshake without knowing the key.
- Weak RC4 keys: With such weak keys input to RC4, a few initial bytes in the output contain recognizable patterns which can be exploited to recover part of the input key. The usage of RC4 in WEP is particularly vulnerable to weak keys, allowing the attacker to recover the entire key quickly. Real implementations show that it requires only 20000 packets to recover the key, which takes less than 1 min in a loaded AP.

4.2.Wi-Fi Protected Access (WPA)

In response to the security flaws in WEP, a new security standard for WLANs, WPA, was released by Wi-Fi Alliance. Today most Wi-Fi products in the market are WPA-compliant, or can be easily upgraded to support WPA. The primary goal of WPA is to amend the known security flaws in WEP yet retain backward compatibility with legacy WEP devices. Thus, WPA is still based on the RC4 stream cipher to reuse the specialized hardware that off-load the computation-intensive RC4 functions from the CPU. By keeping the underlying cryptosystem intact, the new features in WPA can be incorporated into legacy WEP devices through software or firmware updates.

WPA addressed the security flaws in WEP through the following primitives:

- Temporal Key Integrity Protocol (TKIP), a new data encryption protocol that defeats the keystream reuse and weak key attacks.
- message integrity codes (MICs), which defeat the message forgery attacks.
- 802.1x authentication, which achieves strong authentication, authorization, and key management.

TKIP: Similar to WEP, TKIP also XORs the plaintext with a random keystream to obtain the ciphertext. However, it derives the keystream in a way different from WEP. TKIP uses a 128-bit temporal key (TK) and a 48-bit IV. IV is reset to 0 whenever TK is changed, then incremented by one after each transmission. The 48-bit length guarantees that IVs will not be reused with the same TK, as it takes 600+ years to exhaust the space even at 54 Mb/s. As shown in figure(8.3), TKIP uses a two-phase key mixing operation to derive the per-packet keystream, and each phase fixes one particular flaw in WEP. Phase 1 mixes TK with the first 4 bytes of IV and the sender's MAC address, and generates an intermediate key P1K. This prevents keystream reuse due to cross-station collision. Phase 2 takes input P1K with TK and the last 2 bytes of IV to generate a unique 128-bit RC4 key. This decouples the known association between IV and the key, thus preventing exploiting weak keys to recover TK. Finally, the RC4 key is used to generate the keystream, which is then XORed with the plaintext.

MIC: To protect message integrity, WPA uses cryptographic MICs to replace the CRC checksum in WEP. The specific algorithm to compute the MIC is called Michael. The output of the algorithm is a 64-bit tag that serves as the MIC. One major concern in the design of Michael is to reduce the computational overhead. As a result, its defense against message forgery is weaker than one would expect. Although the MIC is 64 bits long, the best-known attack using differential cryptanalysis can reduce its security level to 29 bits, that is, the attacker can forge any message using only 2^{19} MICs.

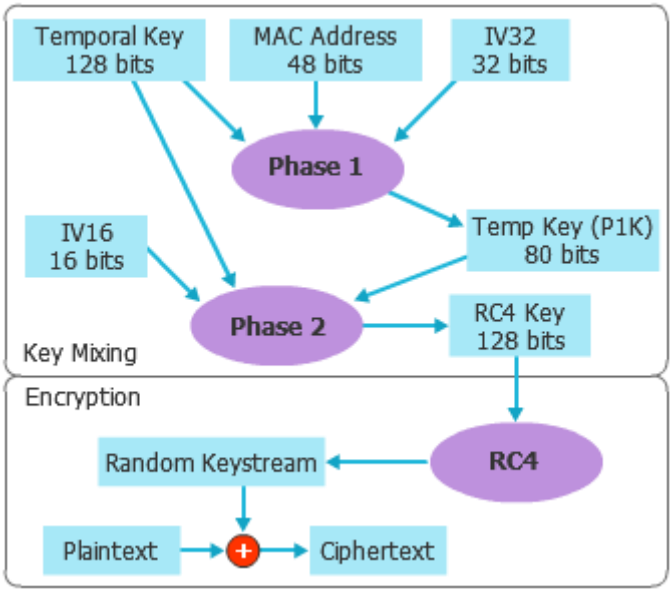


Figure (8.3): Key Mixing and Data Encryption in TKIP

4.3.Robust Security Network (RSN) WPA2 Program

The IEEE 802.11 Task Group proposed RSN (or 802.11i), a new security standard for WLANs. 802.11i was adopted as the next-generation WPA, or so-called WPA2. In fact, WPA was as an interim step in the evolution from WEP to 802.11i, and all its essential features, such as TKIP/Michael, are retained in 802.11i. The new cryptosystem used in 802.11i is the Advanced Encryption Standard (AES). The benefit of using AES is increased security in the long run. However, AES operations typically require a 64-bit coprocessor to improve the performance. As a result, the legacy WEP/WPA devices, especially the APs, can hardly be upgraded to 802.11i without hardware upgrade. The basic primitives in 802.11i include the following:

- TKIP/Michael: TKIP and Michael are retained in 802.11i for data encryption and MIC computation, respectively.
- AES-CCMP: AES in Counter mode with CBC-MAC Protocol (AES-CCMP) is a new protocol for data encryption and MIC computation.
- 802.1x Authentication: 802.1x is used to authenticate the stations and distribute the keying materials.

5.Securing Wireless LANs

The mobility and productivity benefits of 802.11 wireless LANs do not have to put your information assets at risk. While the attention on the pitfalls of WLANs has inspired some enterprises to ban WLANs altogether, many security-conscious enterprises are confidently deploying secure WLANs by implementing the following practical steps to protect their information assets, identify vulnerabilities and protect the network from wireless-specific attacks. We call this a layered approach to security.

Set and Enforce WLAN Policies: Every enterprise network needs a policy for WLAN usage and security. The policy management should define access requirements. Who needs access to what and when? WLAN policies should begin with the basics of forbidding unauthorized access points and ad hoc networks that can circumvent network security. Because many security features, such as the use of WEP or VPNs and open broadcast of SSIDs, are controlled on the access points and stations, policies should be in place to forbid the reconfiguration of access points to alter these features. WLAN security is greatly increased with policies that limit WLAN traffic to operate on set channels, and only during select hours. By establishing a set channel for each access point, all traffic on the other channels can be identified as suspicious activities. A policy that limits WLAN traffic to select hours of operation protects a network from late-night attacks of an intruder in the parking lot connecting to the network or an unscrupulous employee sending sensitive files from the wired network to a wireless network while no one else is around. Although policies are necessary, they can be useless paperweights without enforcement. Similar to the effective discovery of network vulnerabilities, policy enforcement requires 24/7 monitoring of a WLAN.

Configuring the Wireless Access Points Correctly: Wireless access points, usually routers, are the network's central control units and are therefore responsible for their safety. Specifically, the settings you make for this hardware component determine whether an attacker can gain access to your wireless network within a few seconds, or whether it remains just an attempt. These are the most important configuration steps:

Step 1: Create individual administrator access: So that an access point can be configured, firmware needs to be running, which provides a user interface in common internet browsers as soon as you call up the access point's IP address. Access to this interface is achieved through an administrator account with a default username and password. This log-in data is not unique, since it is the same for all devices of the respective model and is also very easy to remember, such as 'admin' (password and username) or '1234'. Change this administrator account log-in information at the beginning of the configuration. You can write it down and store it in a safe place, but do not store it on your computer without proper password storage.

Step 2: Select WPA2 as the encryption method. In order to encrypt your WLAN, you should definitely choose WPA2, since the two predecessors WPA and WEP are outdated and could prove a security risk. Combining or mixing WPA/WPA2 is not recommended either. Instead, use network devices that support WPA2 and do not rely on old encryption methods.

Step 3: Create a secure WLAN password. So far, only password attacks have been known for WPA2, in particular brute force attacks and dictionary attacks are very popular with cyber criminals. The importance of a complex WLAN password therefore cannot be underestimated. Your best bet against decryption algorithms and dictionaries that the tools use is to set up a WLAN key, consisting of as many characters as possible, using both lowercase and uppercase letters as well as numbers and special characters.

Step 4: Specify an unidentifiable network name. WLAN security measures, which primarily serve as your personal protection, are to formulate a non-traceable service set identifier (SSID). The SSID displays the name of your network and is available to all in the signal range. If you are not running a public hotspot, you should avoid personal details that might point to you, your company, or your location. Many consider it all as more secure if they hide the WLAN name, hidden SSID. However, this technique does not fully deter attackers and makes the connection set-up a bit more difficult for legitimate clients. If you hide your WLAN's SSID, it could prevent some devices from seeing the access point, so that they will not be able to connect to it.

Step 5: Turn on automatic firmware updates. So that your WLAN is always secure, it is paramount that the wireless access point's firmware is up to date. As with any software, attackers can take advantage of security flaws. Some access points have an automatic update function for the installed firmware, which you can promptly activate. If this is not the case, you should regularly check whether there are any updates for your device that you can download and install manually.

Discovery and Mitigation of Rogue WLANs and Vulnerabilities: The basis for all WLAN security should start by understanding the environment in which your WLAN operates. Unauthorized "rogue" WLANs, including access points, soft access points (laptops acting as access points), user stations, wireless bar code scanners and printers, represent one of the biggest threats to enterprise network security by creating an open entry point to the enterprise network that bypasses all existing security measures. Because a simple WLAN can be easily installed by attaching an access point to a wired network and a WLAN card to a laptop, these rogue access points generally lack standard security and thus circumvent an enterprise's investment in network security. The default configuration of these devices offer little security and can be easily misconfigured. Intruders can use any insecure wireless station as a launch pad to breach the network. The same insecurity can come from network vulnerabilities originating from improperly configured WLANs. Neighboring WLANs located in the same vicinity as your WLAN also pose risks of the neighboring stations accessing your network and interfering on wireless channels. Freeware, such as NetStumbler and Kismet, and other commercial scanners can survey the airwaves for rogue access points and some network vulnerabilities. A time-consuming effort, this process requires a network administrator to physically walk through the WLAN coverage area looking for wireless data and is limited in effectiveness because it only samples the airwaves for existing threats. New rogue access points and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network. According to wireless security experts, discovery of rogue access points, stations and vulnerabilities is best accomplished with 24/7 monitoring of the WLAN. Continuous monitoring will identify when and where the rogue first appeared, who it connected

to, how much data was exchanged and the direction of traffic in real time. The most secure method is to install a separate set of wireless intrusion-detection sensors.

Intrusion Detection and Protection: Security mangers rely on intrusion-detection and - protection to ensure that all components of WLANs are secure and protected from wireless threats and attacks. While many organizations have already deployed intrusion-detection systems for their wired networks, only a WLAN-focused IDS can protect your network from attacks in the airwaves before the traffic reaches the wired network. The most advanced wireless IDS involves the real-time monitoring of 802.11 protocols. By continuous monitoring of all WLAN attack signatures, protocol analysis, statistical anomaly and policy violations, organizations are able to detect attacks against the WLAN, including identity thefts from MAC spoofing, man-in-the-middle and denial-of-service attacks, and anomalous traffic from unusual off-hours activity or large downloads.

Exercises:

True or False

Question	True	False
1. IEEE 802.11 is a standard for wireless LANs.		
2. Wireless networks, and the wireless devices that use them, introduce a host of security problems over and above those found in wired networks.		
3. Sensors and robots, are not vulnerable to physical attacks.		
4. MAC spoofing occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.		
5. Handheld PDAs pose a security risk in terms of both eavesdropping and spoofing.		
6. The use of 802.1X cannot prevent rogue access points and other unauthorized devices from becoming insecure backdoors.		
7. The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption.		
8. The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions.		
9. You should allow only specific computers to access your wireless network.		
10. Wired networks are far more susceptible to eavesdropping and jamming than wireless networks.		

Multiple Choice Questions

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

2. 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

3. _____ 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

4. 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

5. 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

6. The first 802.11 standard to gain broad industry acceptance was _____.
   A. 802.11i
   B. 802.11a
   C. 802.11g
   D. 802.11b

7. _____ 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

8. "When there is a lack of a central point of control". Which type of Wireless network threat would you classify this under?

A. Man in the middle attack

B. Identity Theft

C. Ad Hoc Networks

D. Non-Traditional Networks

9. Which of these is not a valid Signal-Hiding Technique for Wireless networks?

A. Reducing the signal strength to the lowest level such that it still provides requisite coverage

B. Using directional antennas and signal shielding techniques

C. Installing the wireless access point away from exteriors of the building

D. None of the mentioned

10. "When fraud access points are created to access information such as passwords". Which type of Wireless network threat would you classify this under?

A. Identity Theft

B. Network Injection

C. Man in the middle attack

D. Malicious Association

References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice, 7th edn. Prentice Hall (2017).
2. Hao Yang, F. Ricciato, Songwu Lu and Lixia Zhang, "Securing a Wireless World," in Proceedings of the IEEE, vol. 94, no. 2, pp. 442-454, Feb. 2006.
3. https://www.computerworld.com/article/2567117/five-steps-to-wlan-security---a-layered-approach.html.

Number of the Question	True	False
1	✓	
2	✓	
3		✓
4	✓	
5	✓	
6		✓
7	✓	
8	✓	
9	✓	
10		✓

Number of the Question	Answer
1	A
2	A
3	C
4	C
5	A
6	D
7	D
8	C
9	D
10	D