5.11.2 Wireless Attack Facts

Wireless networks are vulnerable to the following security attacks:

Attack	Description
Deauthentication/Disassociation Attacks	Wireless devices are vulnerable to deauthentication (deauth) and disassociation attacks because the 802.11 standard allows devices to be authenticated with multiple access points at once. ▪ To execute a deauth attack, the attacker pretends to be the wireless router the device is connected to. Then it boots the device from the network. When the user tries to reconnect, the attacker can intercept the user's information. ▪ Disassociation attacks are similar. Instead of kicking a user off the spoofed network and capturing their information when they reverify, disassociation tricks the user into giving the fake router responsibility for forwarding packets.
Rogue Access Point	A *rogue access point* is any unauthorized access point added to a network. Rogue access points can allow the unauthorized capture of credentials and other sensitive information. Attackers also use them to conduct phishing and man-in-the-middle attacks. Examples of rogue access points include: ▪ An attacker or an employee with access to the wired network installs a wireless access point on a free port. The access port then provides a method for remotely accessing the network. ▪ An attacker near a valid wireless access point installs an access point with the same (or similar) SSID. The access point is configured to prompt for credentials, allowing the attacker to steal those credentials or use them in a man-in-the-middle attack to connect to the valid wireless access point. ▪ An attacker configures a wireless access point in a public location, where people unknowingly connect devices. Then he monitors the access point in order to capture sensitive information, such as user names and passwords. Be aware of the following to mitigate and protect your network against rogue access points: ▪ Put access points in separate virtual LANs. ▪ Use site survey tools to identify hosts and APs on the wireless network. ▪ Check connected MAC addresses to identify unauthorized hosts. ▪ Conduct an RF noise analysis to detect a malicious rogue AP that uses jamming to force wireless client to connect to it, instead of legitimate APs. ▪ Analyze wireless traffic to identify rogue hosts. ▪ When you find an unauthorized access point, unplug the Ethernet cable on the access point to disconnect it from the wired network. A rogue access point that is configured to mimic a valid access point is known as an *evil twin*.
Wardriving	With *wardriving*, an attacker scans an area looking for available wireless networks. This is typically accomplished using a high-gain antenna or by driving around looking for unsecured or poorly secured wireless networks. High-gain antennas are easily constructed: ▪ A *cantenna* is constructed using a shaped potato chip can. ▪ A *wokfi* uses a large wok shaped dish. There are two types of wardrivers: ▪ The benign wardriver usually attempts to log information about wireless access points, not collect data from the network. ▪ The malicious wardriver is interested in *piggybacking*, attaching to the network and using services without authorization or permission.
Warchalking	*Warchalking* is similar to wardriving, except the warchalker draws symbols in public places to advertise the existence and status of wireless networks.
Packet Sniffing	*Packet sniffing* (also known as *eavesdropping*, *snorting*, or *snarfing*) is the interception and possible decoding of wireless transmissions. Wireless transmissions are easily intercepted. The wireless network card is set to Monitor mode and picks up all of the packets transmitted on the wireless network. The attacker is not attached to the wireless access point, so it's undetectable. To protect wireless transmissions from packet sniffing, encrypt all data transmitted through, to, and from your access point.
Initialization Vector (IV) Attack	An *initialization vector* (IV) is a seed value used in encryption. The seed value and the key are used in an encryption algorithm to generate additional keys or encrypt data. WEP encryption reuses initialization vectors, which attackers can observe through patterns and crack. This is known as an *IV attack*. For security, the initialization vector should be large, and it should be unpredictable.

Interference	With wireless networks, *interference* is a signal that corrupts or destroys the wireless signal sent by access points and other wireless devices. Non-malicious interference include the following: ▪ Electromagnetic Interference (EMI) is interference caused by motors, heavy machinery, and fluorescent lights. ▪ Radio Frequency Interference (RFI) is interference on the radio channel. It is caused by nearby wireless devices using the same channel, cordless phones, or microwave ovens. Adjacent channels on wireless access points have a small degree of overlap. To avoid interference with other wireless access points within the same vicinity, make sure there is a channel between neighboring wireless access points and the one you are using. For example, if you detect a wireless access point using Channel 5, configure your wireless access point to use any channel other than 4, 5, or 6. Some interference is malicious in nature, designed to disrupt wireless network communications. Malicious interference is sometimes referred to as *jamming*. In a jamming attack, a transmitter is tuned to the same frequency as the wireless network with the same type of modulation. The jamming signal overrides the legitimate wireless network radio signals at the receiving devices. The following list describes different types of jamming signals that can be used to disrupt a Wi-Fi network: ▪ *Spark* jamming is the most effective type of Wi-Fi interference attack. It repeatedly blasts receiving equipment with high-intensity, short-duration RF bursts at a rapid pace. Experienced RF signal technicians can usually identify this type of attack quickly because of the regular nature of the signal. ▪ *Random noise* jamming produces radio signals using random amplitudes and frequencies. While not as effective as a spark attack, the random noise attack is harder to identify due to the intermittent jamming it produces and the random nature of the interference. In fact, this type of signal is frequently mistaken for normal background radio noise that occurs naturally. ▪ *Random pulse* jamming uses radio signal pulses of random amplitude and frequency to interfere with a Wi-Fi network.
Radio-Frequency Identification (RFID)	RFID systems are vulnerable to various kinds of attacks, including the following: ▪ **Eavesdropping**: An attacker uses an RFID reader to listen to conversations between a tag and the intended reader. ▪ **Man-in-the-middle**: An attacker intercepts a signal from an RFID tag, then manipulates the signal before sending it on to the intended recipient. This kind of attack is frequently used to take down a system. ▪ **Denial of service**: An attacker blocks radio signals or jams the system with interfering noise. ▪ **Cloning and spoofing**: An attacker creates a copy of an existing tag, then uses the fake tag to gain access to a secure system.
Bluetooth	Bluetooth is designed to allow devices to communicate within a personal area network (PAN) of close proximity. PAN devices include cell phones, personal digital assistants (PDAs), printers, mice, and keyboards. Bluetooth: ▪ Is designed for longer distances than IR and for lower power consumption. ▪ Requires that devices are in *discovery mode* to find each other and synchronize. ▪ Operates in the 2.4 GHz frequency range and uses adaptive frequency hopping (AFH). Eavesdropping on Bluetooth is difficult because it implements authentication and key derivation with custom algorithms based on the SAFER+ block cipher and uses the E0 stream cipher for encrypting packets. Bluetooth is one of the most secure protocols for mobile device communication, but it is susceptible to the following attacks: ▪ *Bluejacking* is a rather harmless practice that entails an unknown sender sending business cards anonymously to a Bluetooth recipient within a distance of 10-100 meters, depending on the class of the Bluetooth device. The business cards usually include a flirtatious message, used by the attacker to see a visual reaction from the recipient. The attackers sends multiple messages will be sent to the device he thinks there is a chance the recipient will add him as a contact. Bluetooth devices are not susceptible to bluejacking if they are set to *non-discoverable* mode. ▪ *Bluesnarfing* is the use of a Bluetooth connection to gain unauthorized access to an existing Bluetooth connection between phones, desktops, laptops, or PDAs. Bluesnarfing allows access to view the calendar, emails, text messages, and contact lists. Many Bluetooth devices have built-in features to prevent bluesnarfing, but it is still a known vulnerability. ▪ *Bluebugging* gives an attacker access to all mobile phone commands that use Bluetooth technology, such as initiating phone calls, sending and receiving messages, eavesdropping, and reading and writing phonebook contacts. Only by highly-skilled individuals can perform bluebugging. To mitigate the risks with Bluetooth: ▪ Disable Bluetooth completely if not required. Bluetooth and the 802.11b wireless standard both operate on the same frequency range and can lead to signal interference.

	▪ Turn off *discovery mode* if a Bluetooth connection is used on a mobile device.
Near Field Communication (NFC)	Although NFC transmission distances are very short, transmissions are still susceptible to several malicious attacks, including the following: ▪ If a user loses an NFC device, anyone who finds it can access NFC resources as if they were the original owner. ▪ NFC signals can be jammed by malicious interference. ▪ NFC devices and readers are susceptible to man-in-the-middle exploits, where an attacker captures transmissions from the reader and forwards them on to the device, potentially capturing or modifying data in transit. ▪ NFC devices and readers are susceptible to relay attacks, where the attacker captures NFC data in transit and then uses that information to masquerade as the original device.
Wi-Fi Protected Setup	To simplify Wi-Fi setup, many wireless access points implement Wi-Fi Protected Setup (WPS). WPS uses EAP messages between the access point and wireless devices to allow them to connect to the network without the user knowing how to configure network SSIDs and passphrases. Typically, WPS requires the user to perform some action on the wireless device and access point to establish the connection. Common WPS mechanisms include: ▪ Pressing a button on the router and on the wireless device to establish the connection. ▪ Bringing the router and the wireless device into close proximity and using NFC to establish the connection. ▪ Supplying an 8-digit PIN to establish the connection. ▪ Using a USB flash drive to copy Wi-Fi configuration information from the router to the wireless device. Because WPS automates the Wi-Fi association process, attackers can try to exploit the access point to gain unauthorized access to the wireless network. The push-button, USB, and NFC WPS implementations are considered more secure because they require physical access to the access point. However, WPS implementations that only require a PIN are susceptible to brute-force attacks. For this reason, the best security practice is to actually disable WPS functionality in access points that support it.