10.6.4 Wireless Attack Facts

The following table describes security attacks that wireless networks are vulnerable to.

Attack	Description
Rogue Access Point	A *rogue access point* is any unauthorized access point added to a network. Several techniques are used to create a rogue access point. ▪ An attacker or an employee with access to the wired network installs a wireless AP on a free port. The access port then provides a method for remotely accessing the network. ▪ An attacker near a valid wireless AP installs an AP with the same (or similar) SSID. The AP 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 AP. ▪ An attacker configures a wireless AP in a public location, monitors the traffic of users who connect to the wireless AP, and captures sensitive information, such as usernames and passwords. Rogue APs can be used to carry out pharming attacks. In a pharming attack, users are redirected to fake websites that prompt for credentials, allowing the attacker to steal those credentials. To mitigate and protect your network against rogue APs: ▪ Monitor nearby radio frequencies to identify APs broadcasting in your area. ▪ Put APs in separate VLANs and implement some type of intrusion detection to help identify when an attacker sets up a rogue AP or uses a brute force attack to gain access. ▪ When you find an unauthorized AP, unplug the Ethernet cable on the AP to disconnect it from the wired network. A rogue AP that is configured to mimic a valid AP is known as an evil twin.
Data Emanation	Specific threats associated with data emanation (wireless signals extending beyond the intended area of coverage) include the following: ▪ *Wardriving* is a technique that hackers use to find wireless networks. They use detection tools that locate wireless APs within an area even if the SSID broadcast has been disabled. Once a wireless network is detected, it is often easy for hackers to gain access to it, even if they are not physically present in your building or even on your property. ▪ *Warchalking* is when marks that indicate the presence of a wireless network are drawn outside of buildings. Attackers might use these marks to alert others of open or secured wireless networks. Businesses might even use these marks to advertise their free wireless networks. To mitigate and protect your network against data emanation threats: ▪ Do not place APs near outside walls. ▪ Conduct a site survey to identify the coverage area of and optimal placement for wireless APs. This helps prevent signals from going beyond identified boundaries. A site survey uses tools to identify the presence and strength of wireless transmissions. ▪ Implement a Faraday cage or Faraday shield. A Faraday cage is an enclosure that prevents radio frequency signals from emanating out of a controlled environment. It is made of conducting material or a mesh of conducting material that blocks external static electrical fields. Unfortunately, Faraday cages can also prevent cell phone usage. ▪ Encrypt all data transmitted through your AP. ▪ Use firewalls on each network AP.
Packet Sniffing	*Packet sniffing* (also known as eavesdropping) is the interception and decoding of wireless transmissions. Wireless transmissions are easily intercepted. Encrypt all data transmitted through your AP to mitigate threats from packet sniffing.
Interference	With wireless networks, *interference* is a signal that corrupts or destroys the wireless signal sent by APs and other wireless devices. Interference affects the availability of a network because normal communications are made impossible. The following are the most common types of signal interference. ▪ Electromagnetic interference (EMI) is caused by motors, heavy machinery, and fluorescent lights. ▪ Radio frequency interference (RFI) is caused by radio signals using the same radio channel—which can be caused by nearby wireless devices, such as cordless phones or microwave ovens. Most signal interference is caused unintentionally, but some interference is caused intentionally in order to cripple a wireless network. This type of interference is called jamming.

Jamming	*Jamming* is signal interference that is created intentionally by an attacker. Jamming's purpose is to make a wireless network impossible to use. The following are the most common jamming techniques. ▪ *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.
Deauthentication	A *deauthentication* attack is when an attack spoofs your MAC address and then tells your wireless network to disconnect you from the network. Attackers may use a deauthentication attack to stage evil twin or man-in-the-middle attacks.
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 devices to be 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 it uses the E0 stream cipher for encrypting packets. Bluetooth is one of the most secure protocols for mobile device communication, but it is still susceptible to the following attacks. ▪ *Bluejacking* is a harmless practice that anonymously sends business cards 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 to elicit a visual reaction from the recipient. An attacker will send multiple messages to the device if they think there is a chance the user will add him as a contact. Bluetooth devices are not susceptible to bluejacking if they are set to non-discoverable mode. ▪ *Bluesnarfing* is when an attacker gains unauthorized access to an existing Bluetooth connection between phones, desktops, laptops, or PDAs. Bluesnarfing allows access to the calendar, emails, text messages, and contact lists. Many Bluetooth devices have built-in features that 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, listening to phone calls, and reading and writing phonebook contacts. Only highly skilled individuals can perform bluebugging. Implement the following to mitigate Bluetooth risks: ▪ Disable Bluetooth completely if it is not required. Bluetooth and the 802.11b wireless standard both operate on the same frequency range, which can lead to signal interference. ▪ Turn off discovery mode if a Bluetooth connection is used on a mobile device.