8.2.2 Wireless Attack Facts

Because wireless networks communicate using radio waves, they are vulnerable to attack. Common attaacks on wireless networks include Wi-Fi, Bluetooth, and radio frequency identification/near-field communication (RFID/NFC) attacks.

This lesson covers the following topics:

- Wi-Fi attacks
- Bluetooth attacks
- RFID/NFC attacks

Wi-Fi Attacks

Wi-Fi networks are practically everywhere. Many organizations have setup and configured Wi-Fi networks. If not configured properly, these networks can be susceptible to attack. The following table explains common Wi-Fi attacks:

Wi-Fi Attack	Description
Rogue access points (AP)	A rogue AP is any unauthorized AP added to a network. Rogue APs can allow the unauthorized capture of credentials and other sensitive information. Attackers also use this type of attack to conduct phishing and man-in-the-middle attacks. An example of a rogue AP is an employee with access to the wired network installing a wireless AP on a free port. The employee may do this because of poor signal strength. This rogue AP provides access to the network. If the AP has not been secured to the same standards as an official AP, it is likely to be targeted by an attacker. The following actions can be taken to protect against rogue APs: ▪ Put APs 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. ▪ Analyze wireless traffic to identify rogue hosts. ▪ Disconnect any rogue access points you discover.
Evil twin attack	Rogue APs placed by an attacker can be used to run a evil twin attack. In this attack: ▪ The rogue AP is configured to mimic the legitimate network. ▪ The attacker uses a jamming or disassociation attack to knock users off the legitimate network. ▪ When users re-connect to the network, they connect to the attacker's AP. ▪ The attacker can monitor and capture all data that moves through the rogue AP. To protect against this attack, conduct an radio frequency (RF) noise analysis to detect a malicious rogue AP that uses jamming to force

	wireless clients to connect to it, instead of legitimate APs.
Initialization vector (IV) attack	An initialization vector is a seed value used in encryption. The seed value and the key are used in an encryption algorithm to generate additional keys or to encrypt data. Wired Equivalent Privacy (WEP) encryption reuses initialization vectors. The reuse of IVs make it easy for attackers crack them. This is known as an IV attack. Be aware that: - The WEP IV is 24-bits and the key is 40-bits. This allows for approximately 16 million IVs. An IV is repeated at least once every 4096 packets. - Hackers developed programs that flood the network with packets, allowing them to quickly find matching IVs. - Once enough IVs are obtained, the attacker can decrypt the encryption key. - WEP encryption can be cracked in as little as 1-2 minutes. Due to the vulnerabilities of WEP, you should no longer use it. Newer standards such as WPA2 and WPA3 do not use IVs in the encryption process.
Jamming attack	With wireless networks, interference is a signal that corrupts or destroys the wireless signal sent by APs and other wireless devices. Non-malicious interference includes 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 APs have a small degree of overlap. To avoid interference with other wireless APs within the same vicinity, use channels that don't overlap neighboring wireless APs. 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 and the same type of modulation as the wireless network. 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 (radio frequency) 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 and random nature of the interference. In fact, this type of signal is frequently mistaken for 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.
Disassociation/deauthentication attack	Wireless devices are vulnerable to deauthentication (deauth) and disassociation attacks because the 802.11 standard allows devices to be authenticated with multiple APs at once. When a device connects to a wireless network, special unencrypted management packets are sent back and forth. Deauthentication and disassociation attacks take advantage of these packets to disconnect devices from a network. Be aware that: ▪ To execute a deauth attack, the attacker pretends to be the wireless router the device is connected to. The attacker disconnects 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 disconnecting a user, disassociation tricks the user into giving the fake router responsibility for forwarding packets.

Bluetooth Attacks

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 distances longer than infrared (IR) communication and has lower power consumption.
- Requires that devices be in discovery mode to find each other and synchronize.
- Operates in the 2.4 GHz range and uses adaptive frequency hopping (AFH).

Eavesdropping is difficult because Bluetooth implements authentication and key derivation with custom algorithms based on the SAFER+ block cipher. It also 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* looks for nearby devices that are in discovery mode and sends unwanted messages. The attacker is unable to steal any data. This attack is more annoying than harmful.
- *Bluesnarfing* exploits a vulnerability in the object exchange (OBEX) protocol that allows an attacker to pair to the target device. Once paired, the attacker can view the calendar, emails, text messages, contact lists, and other data on the device. Many Bluetooth devices have built-in features to prevent bluesnarfing, but it is still a known vulnerability.

To mitigate the risks of Bluetooth attacks, enable Bluetooth only when needed and make sure discovery mode is turned off except for when pairing devices.

RFID/NFC Attacks

RFID uses radio waves to transmit data from small circuit boards, called RFID tags, to special scanners.

There are two types of RFID tags:

- Active RFID tags have onboard batteries and can send signals over a long distance. Road toll passes and other type passes use active RFID.
- Passive RFID is not powered and relies on the energy of the scanner to transmit data. These tags are seen in ID badges, credit cards, and similar devices.

RFID systems are vulnerable to various kinds of attacks, including:

RFID Attack	Description
Eavesdropping	An attacker uses an RFID reader to listen to conversations between a tag and the intended reader.
Man-in-the-middle (MTM)	An attacker intercepts a signal from an RFID tag, then manipulates the signal before sending it to the intended recipient. This kind of attack is frequently used to take down a system.
Denial of service (DOS)	An attacker blocks radio signals or jams the system with interfering noise.
Cloning and spoofing	An attacker creates a copy of an existing tag and uses the fake tag to gain access to a secure system.

To protect against these attacks, RFID chips often operate at different frequencies. This makes it more difficult for an attacker to find and scan them.

Near Field Communication (NFC) is a newer technology that is built on RFID. NFC allows two-way communication between two devices. The devices must be within a few centimeters of each other. Although NFC transmission distances are very short, transmissions are susceptible to several malicious attacks, including:

- A lost NFC device allows anyone who finds it to access NFC resources.
- 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 reading and/or modifying data in transit.
- NFC devices and readers are susceptible to relay attacks. An attacker can capture NFC data in transit and use the information to masquerade as the original device.