Lesson Proper for Week 10

Security Concerns of Wireless Networking

Wireless networks face different threats than wired networks. Wireless networks do not have physical cabling to secure, so packets literally travel the airwaves and are vulnerable between the transmitter and receiver. If no encryption is used, everything is sent in cleartext, including passwords and confidential data.

This section explains the evolution of wireless security concerns. Wireless communication relies heavily on the Media Access Control (MAC) sublayer of the Data Link layer in the OSI model. MAC frames and MAC addresses play an important role in wireless communication, but they also create vulnerabilities.

Next, you learn about passive and active scanning of wireless networks. Scanning for wireless signals is a valid activity because it allows wireless stations to find and connect to available networks, but these methods are also used to find networks to attack.

The basic authentication methods in IEEE 802.11 networks also cause security problems, so you learn about the inherent vulnerabilities of IEEE 802.11's authentication mechanisms. Then you examine wireless network attacks and major security vulnerabilities, such as the challenge of managing keys and the dangers of using default settings.

Next, you examine common methods for securing wireless networks. Wi-Fi Protected Access (WPA), WPA2, and 802.1x are examples of robust solutions for securing modern wireless networks.

In wireless networks, a wireless device is called a station, which is similar to the term node in wired networks.

IEEE 802.11 Media Access Control: Frames

The MAC sublayer of the OSI model performs many critical functions in a wireless network:

- Discovering wireless access points, channels, and signal strengths
- Joining the wireless network, including authentication and association to the access point
- Transmitting data
- Maintaining the connection

Each access point (AP) has a 0- to 32-byte service set identifier (SSID) that essentially functions as the name of the network. SSIDs separate airwaves into segments so that wireless net- works in the same physical area can operate independently of one another. SSIDs can also be mapped to virtual LANs, so some APs support multiple SSIDs.

When wireless stations communicate, they use MAC frames to locate wireless networks, establish and maintain the connection, and transmit data. All MAC frames contain a control field that identifies the 802.11 protocol version, frame types, and codes that specify wireless configurations. Frames also contain MAC source and destination addresses, a frame sequence number, and a frame check sequence (FCS) for error detection.

The 802.11 standard has three types of MAC frames: management frames, control frames, and data frames. Management frames establish and maintain communications. They are always sent in cleartext, and many contain SSIDs. Even link encryption, such as Wired Equivalent Privacy (WEP), does not encrypt management frames. The security problem with management frames is that anyone who intercepts one can discover the SSID and then have part of the information needed to access the network. Figure 7-1 shows the structure of a management frame.

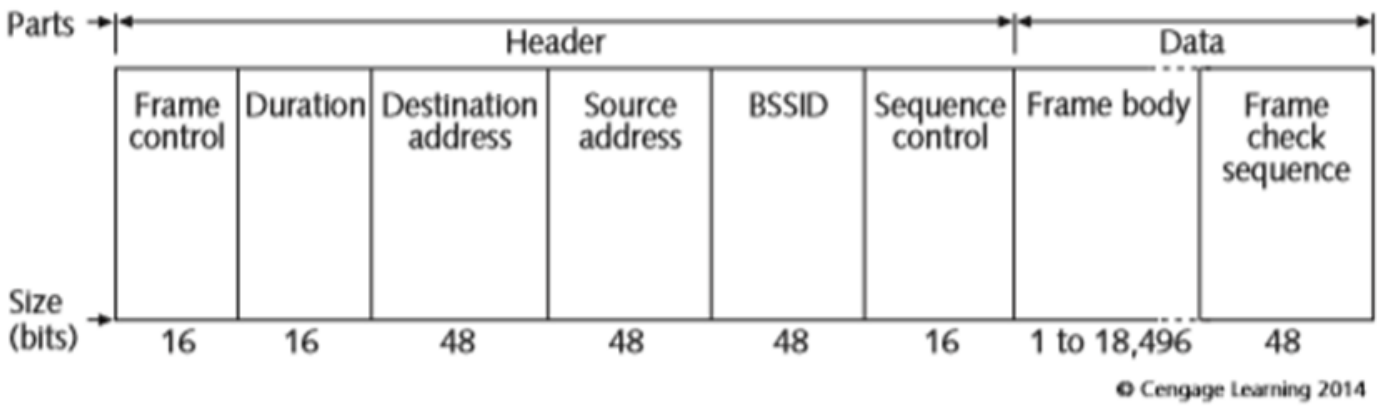

Figure 7-1 An IEEE 802.11 management frame

The following list explains the fields in a management frame:

- Frame control—Information such as the IEEE standard version and whether encryp- tion is used
- Duration—The amount of time in microseconds needed for transmission
- Destination and source address—Source and destination addresses of sending and receiving stations
- BSSID—The basic service set identifier (the network name), a variation of SSID
- Sequence control—The packet's sequence number and fragment number
- Frame body—The data payload
- Frame check sequence—Error detection

Table 7-1 describes common types of management frames.

Frame type	Purpose
Association request	Allows an AP to allocate resources for a wireless station
Association response	Sent by the AP in response to an association request frame; indicates whether the request is accepted or rejected
Reassociation request	Sent to the new AP when a wireless station roams into a different AP coverage area (also called a *"cell"*)
Reassociation response	Sent by the AP in response to a reassociation request frame; indicates whether the request is accepted or rejected
Probe request	Sent by a station when it needs information from another station
Probe response	Sent by a station in response to a probe request frame; indicates capabilities, supported data rates, and other information
Disassociation	Sent by a station to another station if the sender wants to terminate the connection
Authentication	Sent by the AP to determine whether to allow a wireless station to enter the network
Deauthentication	Sent by a station to another station if the sender wants to terminate the connection
Beacon	Sent by an AP to any listening stations to advertise services or information available on the wireless network; beacons contain SSIDs, capabilities, supported rates, and other information about the AP and wireless network

Table 7-1 Management frame types

Reassociation requests and responses might seem confusing because the station does not authenticate again. A station can be authenticated on multiple APs but can be associated with only one at a time. If a station leaves the network on which it is currently authenticated, it must authenticate to the new network. However, moving to a new coverage area does not necessarily mean that the station has changed networks; it simply means that the station has left one AP's coverage area and moved into another.

Control frames help deliver data frames between stations and control access to the medium. Figure 7-2 shows a typical control frame. There are six types of control frames; the following list explains the four most common types:

- RTS—A request to send (RTS) frame is the first step of the two-way handshake before sending a data frame. A station using the RTS/CTS mechanism sends an RTS frame when it wants to transmit data.
- CTS—In response to an RTS frame, a clear to send (CTS) frame gives a station clearance to send. It contains a time value that keeps all other stations from transmitting long enough to give the sending station time to transmit.
- ACK—After receiving a data frame, the receiving station performs error checking. If no error is found, the station sends an acknowledgement (ACK) frame; if no ACK frame is received, the sending station retransmits the frame.
- PS-Poll—A power-save poll (PS-Poll) frame is used when a station has awakened from power-save mode and sees that an AP has frames buffered for it. The station sends this frame to let the AP know it can transmit the buffered frames.

Stations and APs have a configuration parameter called the RTS threshold that indicates whether the RTS/CTS process is used before transmitting. If a station is configured to use RTS/ CTS frames, it transmits an RTS frame requesting access to the medium. After a CTS frame is received in response, the station knows it can transmit safely. All listening stations hear the exchange and hold transmissions long enough for data to be transmitted and to receive an ACK frame indicating success. This process is not foolproof, however. A station that is not listening or not connected to hear the exchange could still transmit during the reserved time.

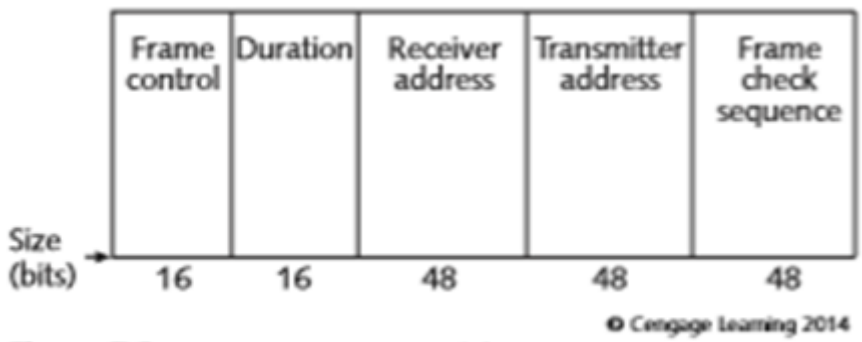

Figure 7-2 An IEEE 802.11 control frame

The following list explains the fields in a control frame:

- Frame control—Information such as the protocol version, frame type, and whether encryption is used
- Duration—The amount of time in microseconds needed for transmission
- Receiver address—The MAC address of the receiving station

- Transmitter address—The MAC address of the transmitting station
- Frame check sequence—Error detection

Data frames carry the TCP/IP datagram, and the payload is encrypted (see Figure 7-3). Data from higher-layer applications, such as printer control data or Web pages, is carried in the data frame body. Data frame fields labeled Address 1, Address 2, Address 3, and Address 4 carry the BSSID, source MAC address, destination MAC address, and address of the transmitter or receiver, respectively.

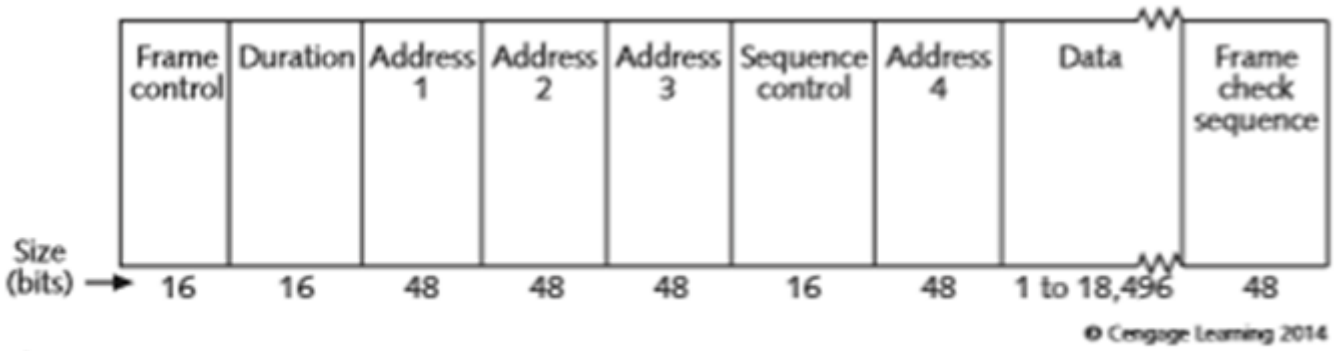

Figure 7-3 An IEEE 802.11 data frame

The following list explains the fields in a data frame:

- Frame control—Information such as the IEEE standard version and whether encryption is used
- Duration—The amount of time in microseconds needed for transmission
- Destination and source address—Source and destination addresses of sending and receiving stations
- BSSID—The basic service set identifier (the network name), a variation of SSID
- Sequence control—The packet's sequence number and fragment number
- Frame body—The data payload (information from higher OSI layers)
- Frame check sequence—Error detection

Unlike MAC addresses and fully qualified domain names (FQDNs), SSIDs are not registered, so two wireless networks could use the same SSID. A station could also have a null SSID that allows it to match all SSIDs. If a beacon frame contains a null SSID, attackers just have to capture frames that contain the correct SSID. You can turn off beaconing for most current APs, but this measure is not very effective; attackers can wait for management or control frames that contain the information they want, or they can spoof (impersonate) management frames and sniff the responses to find information. Sniffing is capturing network traffic during transmission.

In addition, several management frames contain the network's SSID, and management frames are always transmitted in cleartext, even when encryption methods are used. A passive scan can reveal SSIDs to attackers easily, and some APs send beacon frames as often as several times a second, so attackers do not have to wait long to intercept frames that contain SSIDs.

Scanning and Attacks

When a wireless station wants to connect to a wireless network, it begins listening on each available channel for an AP's beacon frame broadcast. This listening process is called passive or active scanning.

In passive scanning, a wireless network interface card (WNIC) listens to each channel for a few packets, and then moves to another channel. Because the station listens without transmitting, its presence is not usually revealed. A WNIC's radio frequency (RF) monitor mode allows passive scanning, although many WNICs have this capability disabled by default in their firmware. In RF monitor mode, the WNIC's equivalent of promiscuous mode in NICs, a WNIC can capture packets without authenticating or associating with an AP or ad-hoc (peer-to-peer) wireless net- work. For this reason, passive scanning is difficult or impossible to detect.

A passive attack uses passive scanning to gather information about a wireless network for later use; this information includes SSIDs, MAC addresses, passwords, and usernames. Wire- less networks are particularly vulnerable to passive attacks, such as sniffing and network reconnaissance. Because transmissions in wireless networks travel over airwaves, attackers simply need to be within range of an unsecured network to intercept packets and then analyze them to get more information for further attacks.

In active scanning, the station sends a probe request frame on each available channel and waits for a probe response frame from available APs. Even after a wireless station is associated with a wireless network, it continues to scan for beacon frames. If a station is disconnected from the net- work, it can reconnect more quickly if it already has the information needed to connect to another AP or station. In general, stations select the strongest signal unless they are configured to connect to a specific AP or other criteria are set. Occasionally, a station connects to the first AP from which it receives a signal.

In active attacks, attackers use several techniques to probe wireless networks in an attempt to gather information. Unlike passive attacks, most active attacks can be detected by network security measures, although some bypass security measures and APs, sending traffic directly to the victim station. Table 7-2 lists some common active attacks; notice that some are denial of service (DoS) attacks.

Many free and commercial tools are available to help intruders automate attacks. Common tools include Aircrack-ng, coWPAtty, WPA Cracker, and WepAttack. However, be careful when you test wardriving software; you could connect to a wireless network inadvertently. If you cause harm, you could face charges whether your actions were intentional or not. As for the legality of simply connecting to an open wireless network, the issue is unclear in many parts of the United States. Some states, such as Florida, have found such connections to be illegal; however, as of this writing, the issue has not been tested in court in most states.

Attack	Method

Jamming (DoS attack)	The attacker floods airwaves with noise to weaken the RF signal and cause the wireless network to stop functioning.
Association flood (DoS attack)	The attacker authenticates several fake stations to send a flood of spoofed association requests, which overflow an AP's association request table. An AP can have up to 2007 concurrent associations before the association request table overflows and refuses further associations.
Forged disassociation (DoS attack)	The attacker sends a forged disassociation frame that contains the spoofed source MAC address of an AP. The target station attempts to reassociate, and the attacker continues to send disassociation frames to prevent reassociation or replies with a reassociation response.
Forged deauthentication	The attacker monitors transmissions to identify target stations. When a data frame or association response frame is captured, the attacker sends a spoofed deauthentication frame that contains the AP's MAC address. To prevent reconnection, the attacker continues to send deauthentication frames for the duration of the attack.
MAC address spoofing	The attacker inserts spoofed values in a frame's sender MAC address field.
Session hijacking	The attacker causes valid users to lose their connections by sending a forged deauthentication or disassociation frame to their stations, for example. The attacker then assumes their identities and privileges by sending their stations' MAC addresses to the AP. The attacker disables users' systems by using a DoS or buffer overflow attack so that their stations cannot reconnect.

Table 7-2 Common active attacks (continues)

Attack	Method
Brute force	The attacker uses a program that attempts every possible key combination by changing one character at a time systematically; this attack is an attempt to decrypt a message and discover the default key.
Dictionary	In an attempt to determine passphrases, the attacker encodes dictionary words in the same way the passphrase was encoded. When the encoding matches, the attacker has found the passphrase.

Table 7-2 Common active attacks (continued)

Some of these attacks take advantage of Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) being used as a wireless access method. With CSMA/CA, stations listen before transmitting. If traffic is already in transmission, stations wait until airwaves are clear before transmitting. In wireless DoS attacks, simply flooding airwaves with transmissions prevents legitimate stations from transmitting.

Wired Ethernet networks use the CSMA/Collision Detection (CD) access method. Stations listen for collisions and wait a random amount of time before transmitting when they detect a collision.

Wardriving and Exploitation of Rogue Devices

In wardriving, a potential attacker drives around with a laptop and WNIC in RF monitor mode to detect unsecured wireless signals. Wardrivers can use inexpensive hardware and free software to access an unsecured wireless network easily, regardless of whether it is part of an enterprise network or home network.

A myth has developed that wardrivers are simply hijacking a connection, but in fact they are stealing information, violating data privacy, and possibly using their access to cause malicious damage.

Rogue devices are wireless devices that employees connect and use without authorization or verified configurations. Many administrators consider rogue devices to be a minor problem, but any unauthorized device represents a security vulnerability that can be exploited. In addition, rogue devices are usually configured poorly, so attackers can often locate them quickly and easily.

For example, Betty is an accounts payable manager who wants a mobile connection in the file room because she often reviews and files paperwork or reconciles accounts there. If she could take her laptop with her, she would not have to haul files between her office and the file room. She asked the IT Department to set up a wireless connection for her, but the request was refused. Undeterred, Betty researches wireless connections and finds out that she needs only a wireless router and WNIC. Her laptop has an onboard WNIC, so she buys an inexpensive wire- less router. She follows the simple instructions to attach the router, and then uses the Windows 7 wizard to configure the WNIC and connect to the corporate network. She thinks that the IT Department was too lazy to help her because the wireless connection was not hard or time consuming to set up, and she is satisfied that she was technically savvy enough to do it herself.

The next morning, a wardriver is cruising around the neighborhood. He looks at his laptop and sees that his antenna has detected a WLAN broadcasting advertisements as “linksys.”

He knows immediately that he has detected a wireless router configured with default settings. His open-source software tells him that the router is broadcasting unencrypted packets, so he connects to it and starts capturing packets. He examines the packets and finds what he is looking for: a valid username and password. With this information, he can probably gain full access to the network and steal sensitive information. With a little more effort, he can disable software, infect the network with a virus, and delete or corrupt data.

This situation happens every day, but companies often do not realize that well-intentioned employees are a common source of wireless security breaches. Worse, the IT Department might not have configured wireless network security and auditing correctly, so rogue devices often go unnoticed until a breach is discovered. According to a 2011 survey, 19% of wireless networks use the obsolete and unsecure WEP standard, 11% use default configurations, and 6% have no security measures at all. While these statistics show an improvement over similar surveys in the previous decade, the proliferation of wireless devices makes lax security mea- sures a headache for security professionals and makes intrusions easy for attackers.

Although it might seem that Betty is solely responsible for any harm that occurs to the net- work, the IT Department shares responsibility. Too often, IT personnel are unresponsive or abrupt with users. Had an IT Department employee politely explained to Betty why her request could not be accommodated, she might not have taken steps to set up her own wire- less connection. Unfortunately, she was not as knowledgeable as she thought she was, so her laptop's connection was not secured correctly. A comprehensive security-training program that included information about wardriving and rogue devices would have helped prevent Betty's actions. IT professionals should treat users with respect to help ensure that network security is maintained. If you work in IT and maintain a good working relationship with users, they are usually willing to follow security procedures. If you refuse to help them, they might circumvent the procedures you have set up.

Wireless Man-in-the-Middle Attacks

In a man-in-the-middle (MITM) attack, attackers intercept the transmissions of two communicating nodes without the users' knowledge. The transmissions can be modified and then forwarded to the intended destination, blocked from being delivered, or simply read and passed on. Most wired networks take countermeasures to reduce the risk of MITM attacks, but wireless networks provide new opportunities to use this attack method. A wireless MITM attack follows the same general procedure as on a wired network, but attackers often set up a fake AP to intercept transmissions and make stations think they are connecting to an authentic AP. Figure 7-4 shows a typical wireless MITM attack.

Secure WLAN Implementation

Association with a Wireless Network

To access services and resources, a station must be associated with an AP (in infrastructure mode) or another station (in ad-hoc mode). Association is a two-step process. First, a station listens for beacon frames to locate a network to join and then goes through the authentication process; a station cannot be associated without being authenticated first. Second, the station sends an association request frame. If the AP accepts, it reserves memory space for the station and sends back an association response frame that contains the association ID and connection information, such as supported data rates. A station can be authenticated on several APs simultaneously, but it can be associated with only one network at a time.

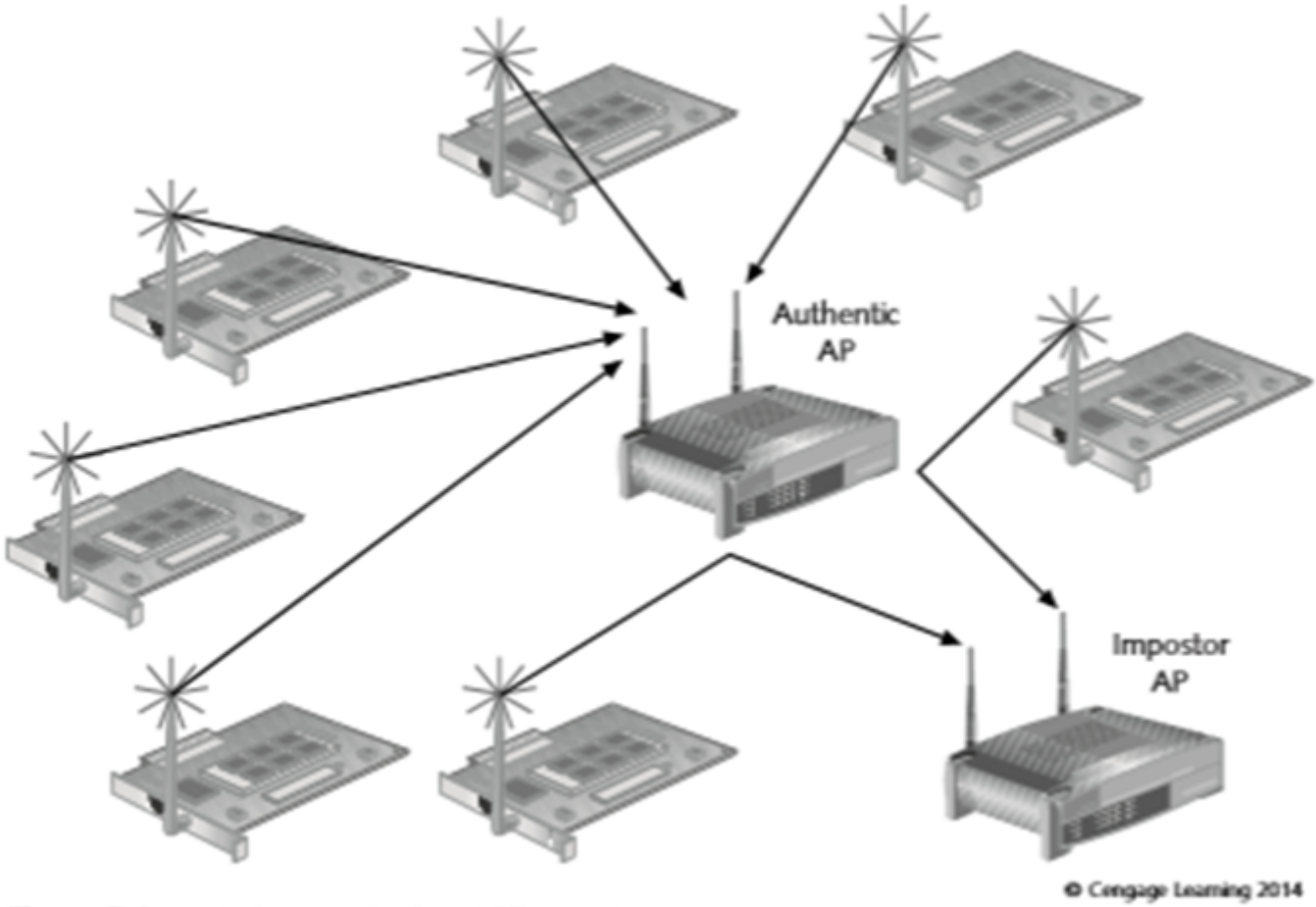

Figure 7-4 A wireless man-in-the-middle attack

Wireless Authentication

When a wireless station wants to connect to a network, it authenticates to an AP or another station first in a process called IEEE 802.11 authentication. A key difference between wire- less and wired networks is that the wireless station, not the user, is authenticated before being connected to the network. To access resources, users are then prompted to authenticate after the connection has been made. However, the AP typically does not perform user authentication; that process is handled by a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) server, directory services, or another means of network authentication.

Early 802.11 standards provide two basic authentication methods: open system authentication and shared key authentication. In open system authentication, a station is authenticated without further checking as long as it has an SSID that matches the network it is attempting to join (see Figure 7-5). In ad-hoc mode, which is used in a peer-to-peer network, one station sends an authentication frame to another and receives a frame indicating recognition. In infrastructure mode—another term for a BSS configuration, with APs connecting stations—a station transmits its request to the AP and is authenticated as long as it has the correct SSID. Open system authentication provides little security because SSIDs are transmitted in management frames in cleartext. Attackers can easily use passive scanning to find this information from other authenticated stations or from the AP if it is broadcasting beacon frames.

Figure 7-5 Open system authentication

Shared key authentication uses a standard challenge-response process with shared key encryption. A wireless station sends an authentication frame to an AP, which returns an authentication response frame that contains the challenge text. The station encrypts the text with its shared key and returns it to the AP. Using its own copy of the shared key, the AP decrypts the text and compares it to the original challenge text. If they match, the AP sends another authentication frame with the results, and the station is authenticated. If they do not match, the station's connection attempt is rejected.

A single shared key is distributed to all stations on a wireless network before they can communicate (see Figure 7-6). The IEEE standards do not specify any mechanisms for key management, so vendors, administrators, developers, and others must devise their own key management schemes. Managing shared keys effectively is a challenging aspect of securing wireless transmissions. Shared key authentication is also considered weak if it uses WEP for encryption. Attackers can use passive scanning to capture packets and crack the shared key; after they have the key, they can be authenticated to the network easily and then launch attacks.

The initial 802.11 standard included WEP and outlined several of the following crypto- graphic objectives, but did not specify how to achieve them:

- Efficiency—The encryption algorithm must be efficient enough to be used in hardware or software.
- Exportable—U.S. Department of Commerce security guidelines must be met so that WEP-enabled devices can be exported outside the United States.
- Optional—WEP must be an optional feature.
- Self-synchronizing—Each packet must be encrypted separately so that a single lost packet does not result in all packets being unreadable.

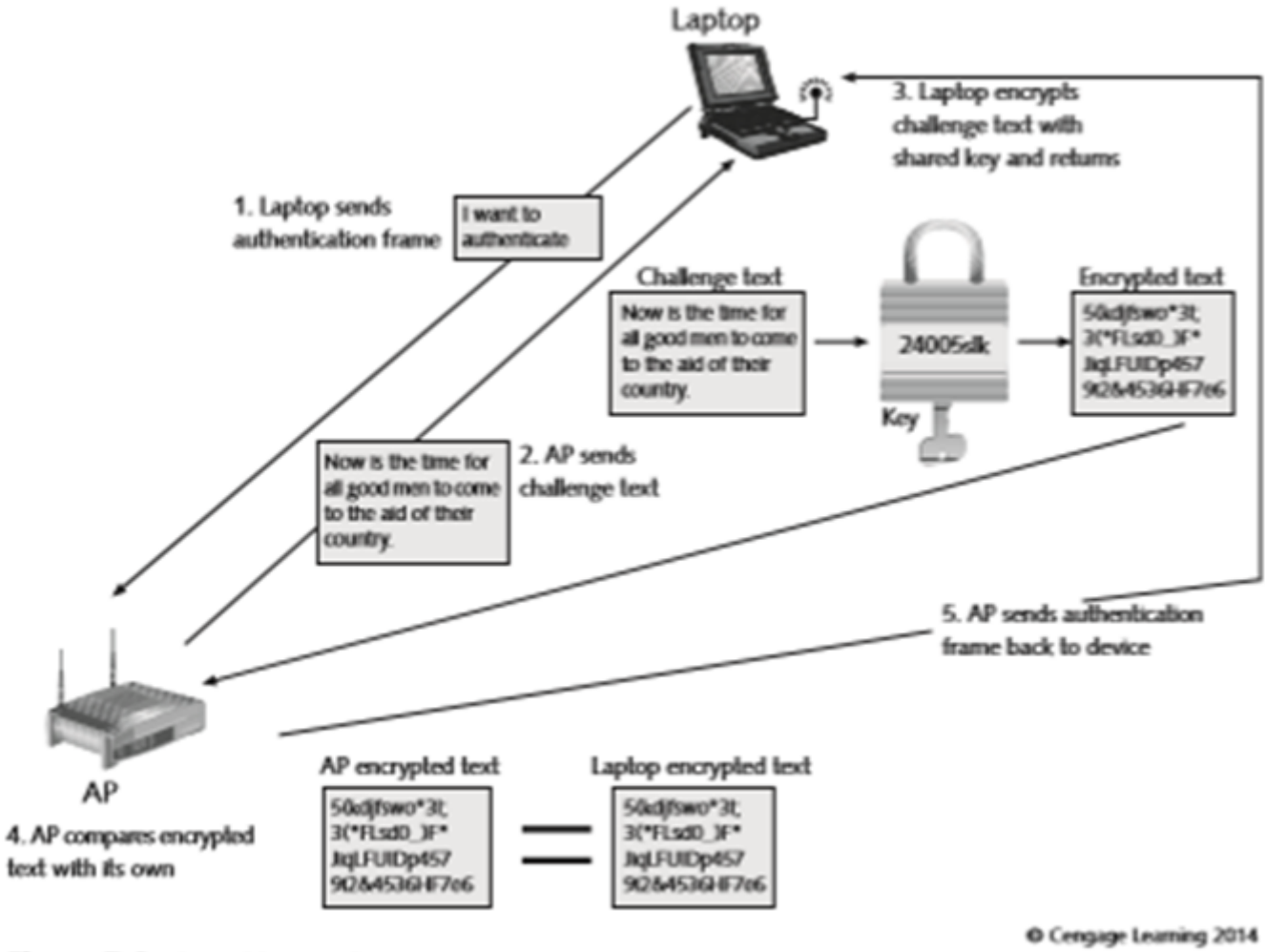

Figure 7-6 Shared key authentication

Shared key encryption in WEP uses the Rivest Cipher version 4 (RC4) encryption algorithm, which allows keys of up to 128 bits. The 802.11 standard uses a 40-bit or 104-bit key with a 24-bit initialization vector (IV) added to the beginning of the key. The IV initializes the key stream generated by the RC4 algorithm and is transmitted in cleartext.

To understand WEP's weaknesses, you need to understand IV vulnerabilities. The IV is part of the RC4 encryption key, and because it is transmitted in cleartext, it gives attackers 24 bits of the key. The IV is a short stream by cryptographic standards, and reusing the same key results in keys that repeat after a short time. All users use the same key, so capturing enough packets to crack the key and decrypt transmissions is not difficult.

Often, the IV starts at 0 and increments by 1 each time a key is generated, so not only does it repeat, it does so in a predictable pattern. Because the IV is a 24-bit value, only 16 million combinations are possible. Therefore, in a busy network, the IV can reinitialize and start over at 0 in about 6 hours. After enough packets have been captured, attackers can crack the key with a brute-force or dictionary attack.

Because the challenge text in shared key authentication is sent in cleartext, attackers can capture it along with the IV and then capture the challenge response. With this information, they can crack the key. Even though the RC4 specifications make it clear that keys should never be reused, inevitably they are in WEP.

WEP provides adequate protection against casual users with no ill intent, but not against attackers who are determined to gain access. Dynamic WEP, a newer version, offers slightly better protection because it rotates keys frequently, which solves the IV problem. It also uses different keys for broadcast and unicast traffic and changes them frequently. Dynamic WEP requires minimal effort to set up, but it is not used much because it provides only a partial solution. Another option is WEP2, which was developed to address some vulnerabilities in WEP. WEP2 uses a 128-bit key and Kerberos authentication. Although these enhancements help, WEP2 is no more secure than WEP and is not used widely.

WEP is often disabled to increase throughput. Even though it does not provide much security, you should still make sure it is enabled as a first line of defense to prevent casual users from connecting.

Default WEP Keys

Even though the 802.11 standard states that APs and wireless stations can hold up to four keys simultaneously (see Figure 7-7), only one is chosen as a station's default key to encrypt messages for transmission. The default key does not have to be the same on every station, but the same key must be used for both encryption and decryption. Each station must contain the key used for encryption to decrypt messages. For example, if a sending station uses Key 3 for encryption, the receiving station must use its copy of Key 3 to decrypt the message.