Hands-On Ethical Hacking and Network Defense, Edition 4

Chapter 11: Hacking Wireless Networks

Module Objectives

- By the end of this module, you should be able to:
  - Explain wireless technology
  - Describe wireless networking standards
  - Describe the process of authentication
  - Describe wardriving
  - Describe wireless hacking and tools used by hackers and security professionals

Understanding Wireless Technology

- For a wireless network to function, you must have:
  - The right hardware and software
  - Technology that sends and receives radio waves
- Wireless technology is part of daily life
  - Baby monitors
  - Cell phones and smartphones
  - Global positioning system (GPS) devices
  - Keyless entry, remote controls, and garage door openers
  - Two-way radios
  - Bluetooth speakers

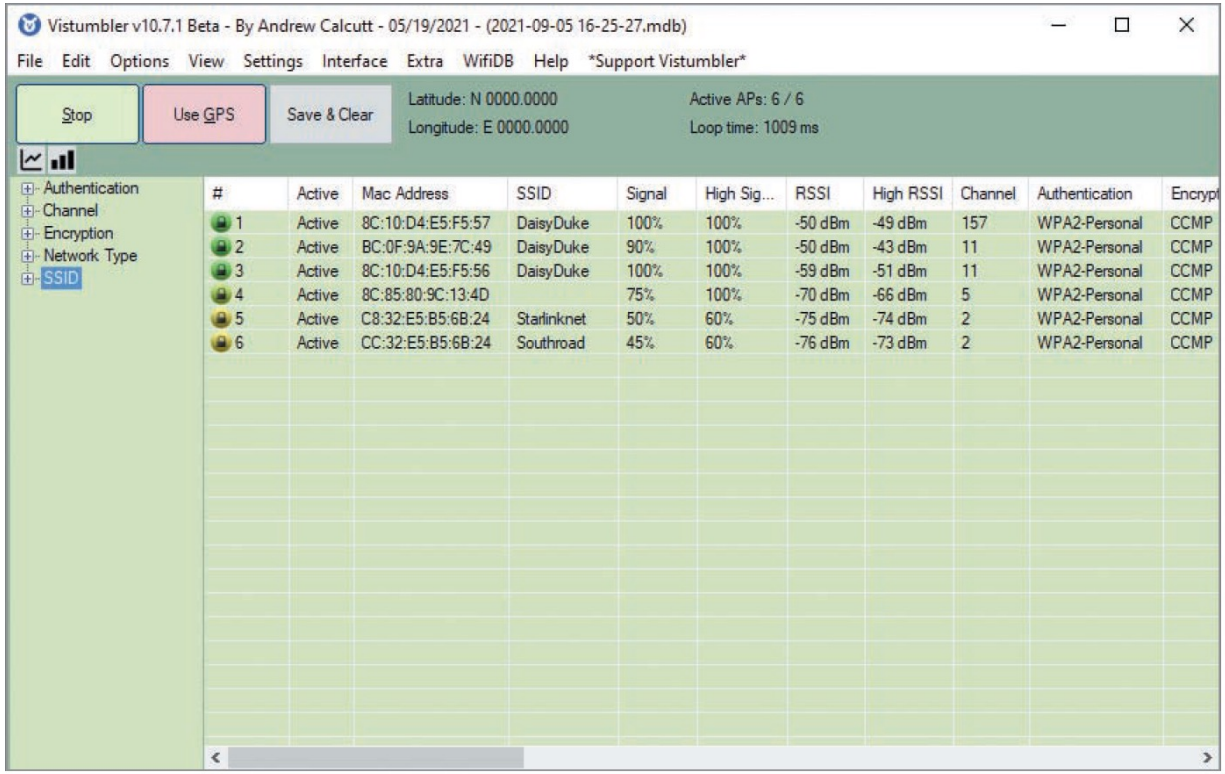
Components of a Wireless Network (1 of 3)

- Only a few basic components:
  - **Wireless network interface cards (WNICs)**
    - Transmit and receive wireless signals
  - Access points (APs)
    - The bridges between wired and wireless networks
  - Wireless networking protocols
  - A portion of the RF spectrum

Components of a Wireless Network (2 of 3)

- **Access point (AP)**
  - Radio transceiver that connects to a network via an Ethernet cable
  - Links a **wireless LAN (WLAN)** to a wired network
    - Not all connect to a wired network
    - Most companies use WLANs connected to the company's wired network topology
  - Point where RF channels are configured
  - Enables users to connect to a LAN
    - Using wireless technology
    - Available only within a defined area

Components of a Wireless Network (3 of 3)



Source: GNU General Public License (GNU GPL)

Figure 11-1 AP channels detected

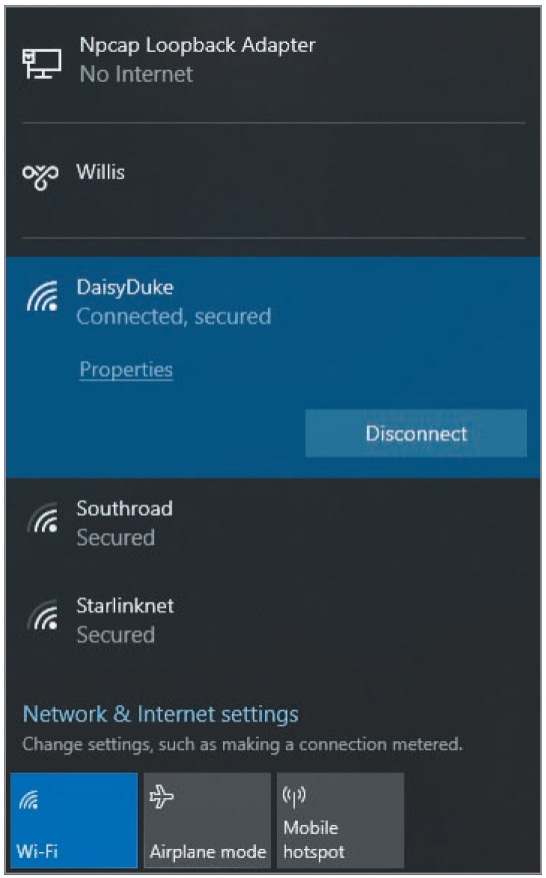
Service Set Identifiers (1 of 4)

- SSID
  - Name used to identify a WLAN
- Configured on the AP
  - Unique 1- to 32-character alphanumeric name
  - Case-sensitive

Service Set Identifiers (2 of 4)

- To access the WLAN the AP connects to, wireless-enabled computers must configure with the same SSID as the AP
  - The SSID name is attached to each packet to identify it as belonging to that wireless network
  - AP usually broadcasts SSID several times a second
    - Users with WNICs can see a display of all WLANs within range of the AP's signal

Service Set Identifiers (3 of 4)



Source: Microsoft Windows

Figure 11-2 SSIDs advertised to a Windows computer

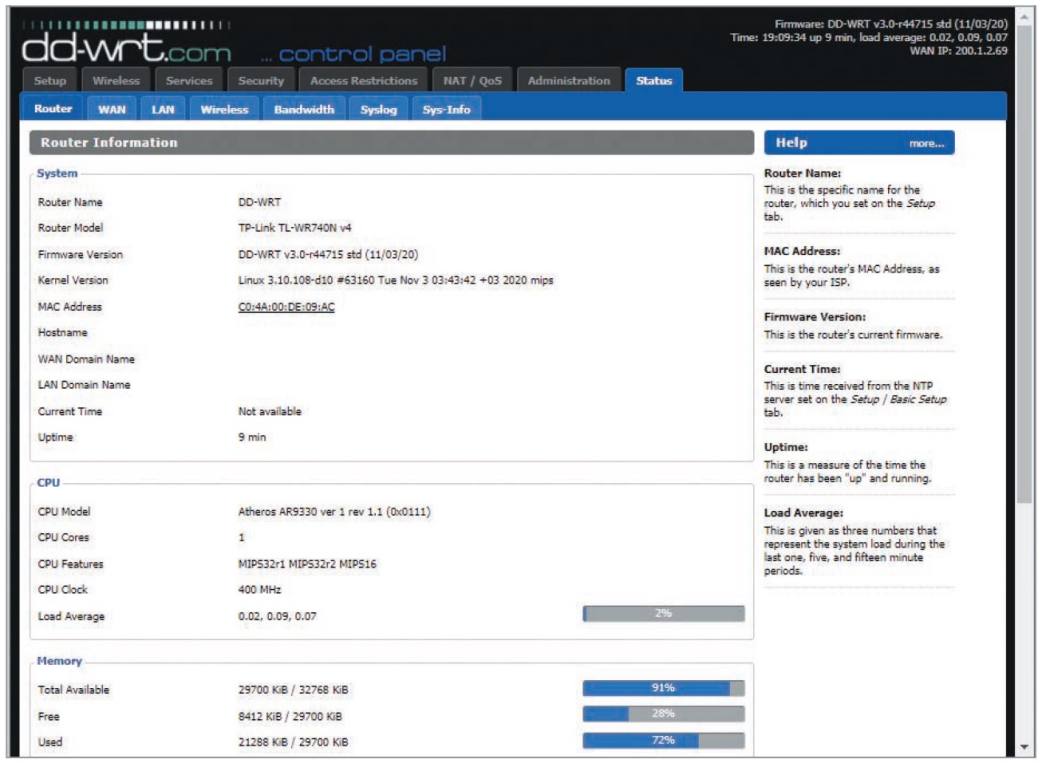
Service Set Identifiers (4 of 4)

- Vendors
  - Many have SSIDs set to a default value that companies never change
- As a security professional, you must research constantly
  - Wireless hackers can attempt to guess SSID
  - Verify your clients are not using a default SSID
  - A default SSID
    - Tells an attacker that the target AP is out of date

Configuring an Access Point (1 of 4)

- Configuring an AP varies
  - Depending on the embedded OS supplied by the manufacturer
  - Users can access the software through a web browser
    - Because the AP has an embedded OS supporting a web server
- Accessing and reconfiguring a wireless router running dd-wrt:
  - Enter the IP address in a web browser
  - Provide the user logon name and password
  - After a successful logon, click the Status tab
  - Click the Wireless tab to display the Wireless Interface
  - Click the Wireless Security tab to configure security

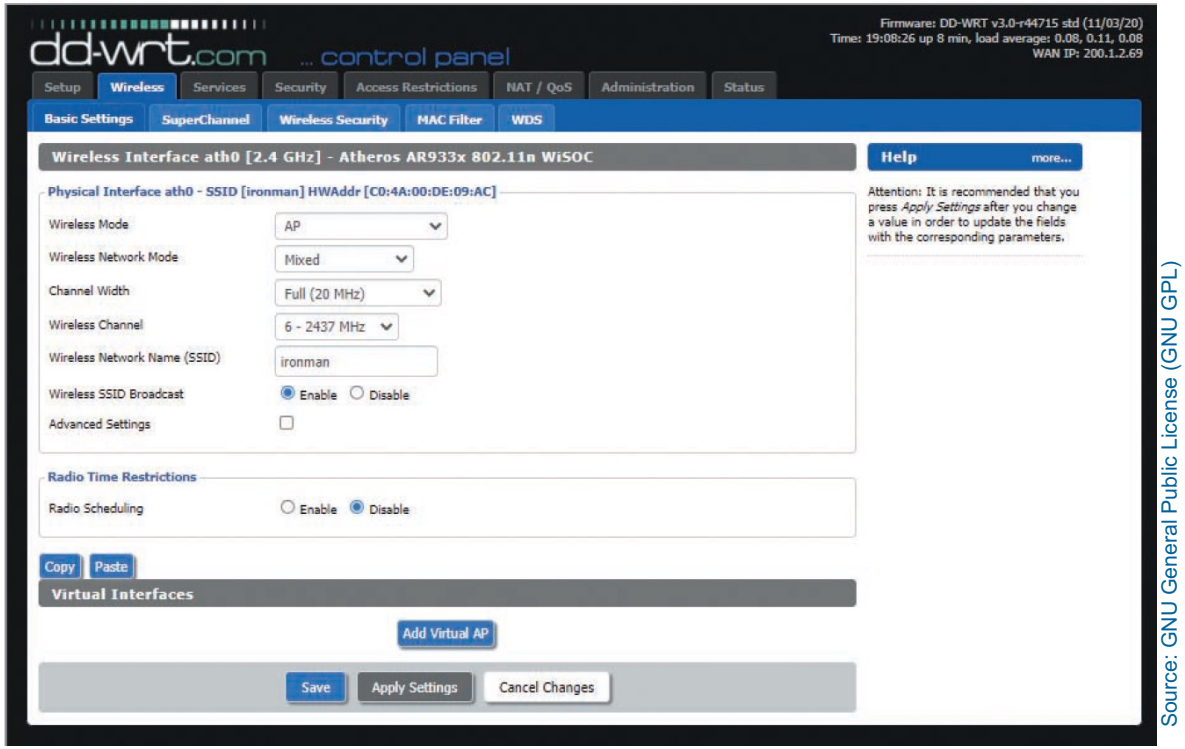
Configuring an Access Point (2 of 4)



Source: GNU General Public License (GNU GPL)

Figure 11-3 Viewing status information in dd-wrt

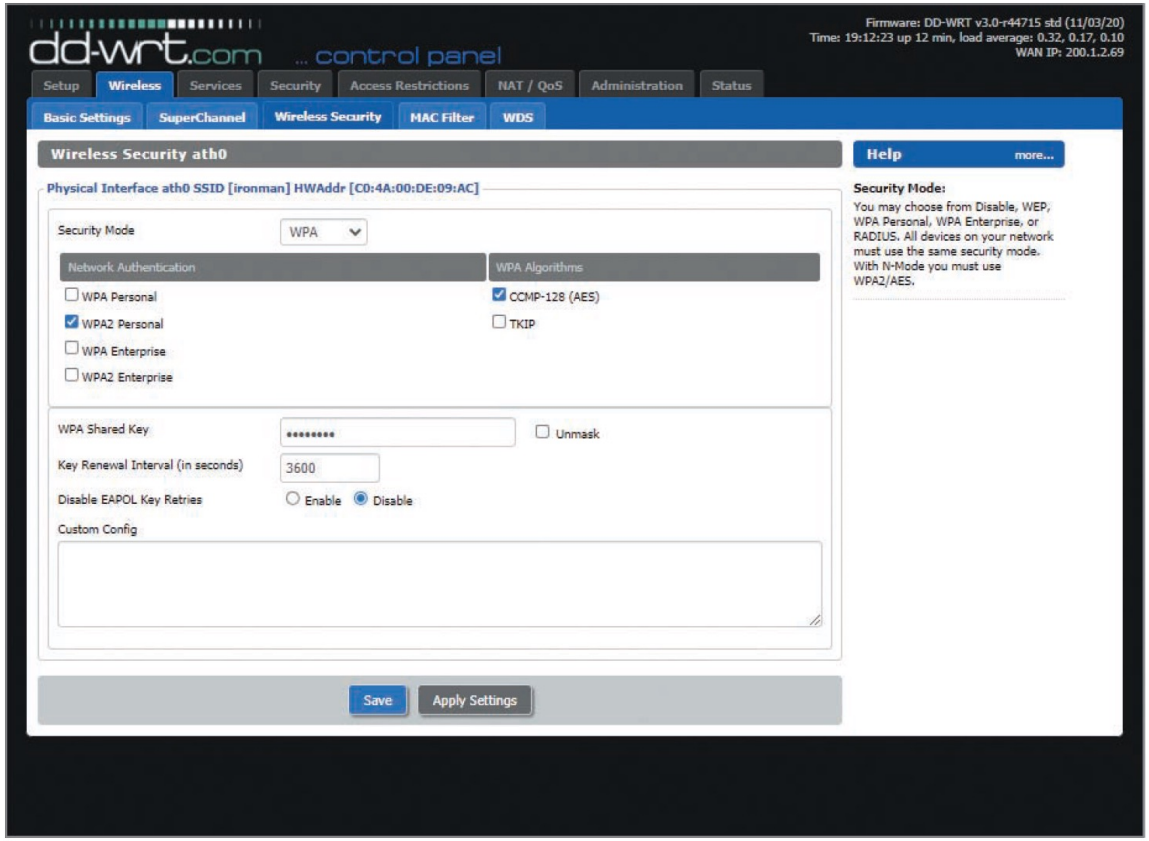
Configuring an Access Point (3 of 4)



Source: GNU General Public License (GNU GPL)

Figure 11-4 Basic wireless configuration in dd-wrt

Configuring an Access Point (4 of 4)



Source: GNU General Public License (GNU GPL)

Figure 11-5 Configuring wireless security in dd-wrt

Wireless NICs

- For wireless technology to work, each node or computer must have a WNIC
  - WNIC converts radio waves into digital signals the computer understands
- There are many WNICs on the market
  - Be careful deciding which one to purchase
  - Some tools require certain specific brands

Understanding Wireless Network Standards

- Standard
  - Set of rules formulated by an organization
- **Institute of Electrical and Electronics Engineers (IEEE)**
  - Has standards specifying maximum cable length in an Ethernet network
  - Sets rules to follow for wireless networks
  - Working groups (WGs) of the IEEE are formed to develop new standards
    - IEEE Project 802: Developed to create LAN and WAN standards
  - WG names are assigned numbers
    - Example: 11 for the Wireless LAN group
    - Letters denote approved projects
      - Example: 802.11a or 802.11b

The 802.11 Standard

- The first wireless technology standard
- Defined specifications for wireless connectivity as 1Mbps and 2Mbps in a LAN
- Applied to the Physical layer of the OSI model
- Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD (collision detection, used in Ethernet)
  - This is because radio signals can mix and cause a potential signal collision
- Wireless LANs
  - Don’t have an address associated with a physical location
    - An addressable unit is called a **station (STA)**

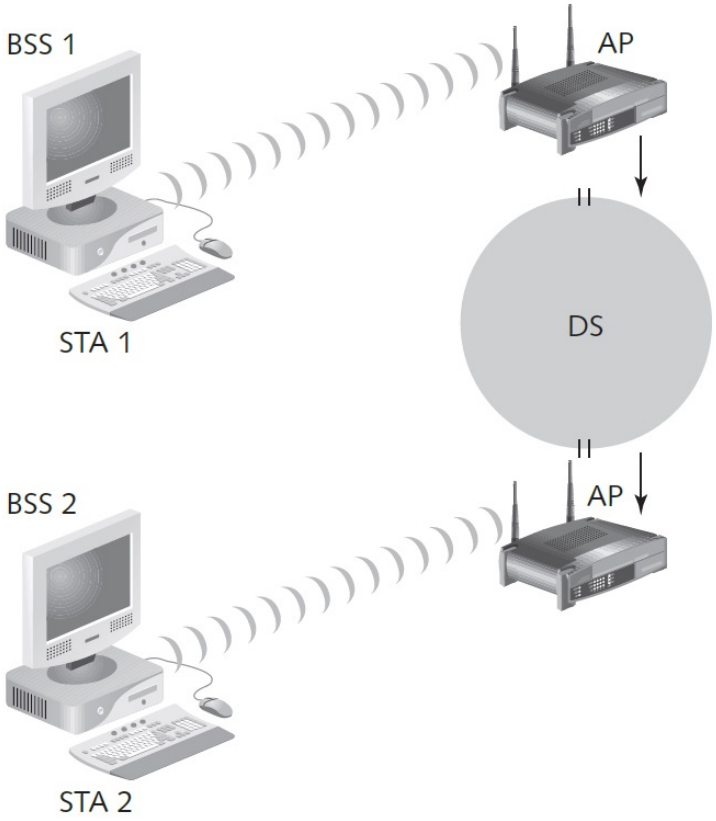
The Basic Architecture of 802.11 (1 of 5)

- 802.11 uses a **basic service set (BSS)** as its building block
  - BSS
    - Collection of devices that make up a WLAN
- **Basic service area (BSA)**
  - The coverage area an AP provides
- A WLAN running in **infrastructure mode**
  - Always has one or more APs
- **Ad-hoc network**
  - An independent WLAN without an AP

The Basic Architecture of 802.11 (2 of 5)

- As long as a station is within its BSA, it can communicate with other stations in the BSS
- To connect two BSSs:
  - 802.11 requires a distribution system (DS) as an intermediate layer
    - BSS 1 connects to the DS, which in turn connects to BSS 2
    - Data moves between a BSS and the DS through the AP

The Basic Architecture of 802.11 (3 of 5)



Source: Cengage

Figure 11-6 Connecting two wireless remote stations

The Basic Architecture of 802.11 (4 of 5)

- IEEE specifications
  - Define the operating frequency range of 802.11
    - United States: The range is 2.4 to 2.4835 GHz
- Each frequency band contains **channels**
  - A channel breaks up the band into smaller frequency ranges
  - The 802.11 standard defines 11 channels in the 2.4 to 2.462 GHz range
    - If channels overlap, interference could occur

The Basic Architecture of 802.11 (5 of 5)

- The length of a sound wave is measured from the peak of one wave to the next
  - A sound wave's **amplitude** (height) and **frequency** determine its volume and pitch
    - Frequency
      - Rate at which sound waves repeat
    - Cycle
      - Completion of a repeating pattern of sound waves
    - Bands
      - Different frequencies used by different technologies to transmit sound

Frequency Bands

Frequency	Range	Wavelength
Extremely low frequency (E L F)	3 to 30 Hz	100,000 km to 10,000 km
Super low frequency (SLF)	30 to 300 Hz	10,000 km to 1000 km
Voice frequency (VF) or ultra-low frequency (ULF)	300 Hz to 3 KHz	1000 km to 100 km
Very low frequency (VLF)	3 to 30 KHz	100 km to 10 km
Low frequency (LF)	30 to 300 KHz	10 km to 1 km
Medium frequency (MF)	300 KHz to 3 MHz	1 km to 100 m
High frequency (HF)	3 to 30 MHz	100 m to 10 m
Very high frequency (VHF)	30 to 300 MHz	10 m to 1 m
Ultra high frequency (UHF)	300 MHz to 3 GHz	1 m to 10 cm
Super high frequency (SHF)	3 to 30 GHz	10 cm to 1 cm
Extremely high frequency (EHF)	30 to 300 GHz	1 cm to 1 mm

An Overview of Wireless Technologies (1 of 2)

- **Infrared (IR) technology**
  - Restricted to a single room or line of sight
    - Infrared light can't be seen by the human eye
      - Cannot penetrate walls, ceilings, or floors
- **Narrowband**
  - Uses microwave radio band frequencies to transmit data
  - Commonly used in:
    - Cordless phones
    - Garage door openers

An Overview of Wireless Technologies (2 of 2)

- Spread spectrum
  - To move over radio waves, data must be modulated on the carrier signal or channel
    - **Modulation**
      - Defines how data is placed on carrier signal
    - Spread spectrum modulation
      - Data is spread across a large-frequency bandwidth instead of traveling across just one frequency band
  - Uses the following methods:
    - Frequency-hopping spread spectrum (FHSS)
    - Direct sequence spread spectrum (DSSS)
    - Orthogonal frequency division multiplexing (OFDM)
    - Orthogonal frequency division multiplexing Access (OFDMA)

Additional IEEE 802.11 Projects (1 of 5)

- 802.11b (referred to as Wi-Fi)
  - Operates in the 2.4 GHz band
  - Throughput increased to 11 Mbps from the 1 or 2 Mbps of the original 802.11
  - Allows for 11 separate channels to prevent overlapping signals
    - Only three channels (1, 6, and 11) can be combined without overlapping and creating interference
  - Introduced Wired Equivalent Privacy (WEP)

Additional IEEE 802.11 Projects (2 of 5)

- 802.11a standard
  - Has a different operating frequency range from 802.11 and 802.11b
  - Operates in three distinct bands in the 5 GHz range
  - Throughput increases to 54 Mbps
- 802.11g standard
  - Operates in the 2.4 GHz range
  - Because it uses a different modulation, it uses the OFDM method
    - Increases the throughput to 54 Mbps

Additional IEEE 802.11 Projects (3 of 5)

- 802.11i standard
  - Introduced Wi-Fi Protected Access (WPA)
  - Corrected many security vulnerabilities in 802.11b
  - Most important standard for security professionals
- 802.11e standard
  - Has improvements that address the problem of interference
    - When interference is detected, signals can jump to another frequency more quickly
- 802.11n standard
  - Operates in the same frequency and uses same encoding as 802.11g
  - Uses multiple antennas and wider channels
    - Increases the throughput to 600 Mbps

Additional IEEE 802.11 Projects (4 of 5)

- 802.11ac standard
  - Uses the 5 GHz band
  - Allows for higher throughput (up to 1 gigabit per second)
- 802.11ad standard
  - Dubbed “WiGig”
  - Allows for transfer rates up to 7 gigabits per second over the 2.4 GHz, 5 GHz, and 60 GHz bands

Additional IEEE 802.11 Projects (5 of 5)

- 802.11ah standard
  - Targets lower energy consumption
  - Creates extended-range Wi-Fi networks
- 802.11aj standard
  - Known as the China Millimeter Wave
  - Goal: Maintain backward compatibility with 802.11ad
  - Technology uses the 45 GHz and 60 GHz spectrums uniquely available in China
- The 802.11x standard
  - Branded as Wi-Fi 6
  - Replaces 802.11ac as the de facto wireless standard
  - Wi-Fi 6 maxes out at 10 Gbps, uses less power, is more reliable in congested environments, and supports better security

Additional IEEE 802 Standards (1 of 2)

- 802.15 standard
  - Addresses networking devices in one person's workspace
    - **Wireless personal area network (WPAN)**
    - Bluetooth is a common example
- 802.16 standard
  - Covers wireless **metropolitan area networks** (**M A Ns**)
  - Defines the Wireless M A N Air Interface for wireless M A Ns
  - Addresses the limited distance available for 802.11b WLANs
  - **Worldwide Interoperability for Microwave Access (WiMAX)**
    - Most widely used implementation of wireless M A N technology

Additional IEEE 802 Standards (2 of 2)

- 802.20 standard
  - Another M A N standard
  - Known as **Mobile Broadband Wireless Access (MBWA)**
  - Addresses wireless M A Ns for mobile users
    - Traveling in trains, subways, or cars at speeds up to 150 miles per hour
  - iBurst
    - Most common implementation of MBWA
    - Used widely in Africa and Asia

Summary of Approved Wireless Standards (1 of 2)

Standard	Frequency	Maximum rate	Modulation method
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11n	2.4 GHz & 5 GHz	600 Mbps	OFDM
802.11ac	5 GHz	1 Gbps	OFDM
802.11ad	2.4 GHz, 5 GHz, & 60 GHz	7 Gbps	OFDM
802.11ah	900 MHz	347 Mbps	OFDM
802.11aj	45 GHz & 60 GHz	15 Gbps	OFDM

Summary of Approved Wireless Standards (2 of 2)

Standard	Frequency	Maximum rate	Modulation method
802.11ax	2.4 GHz & 5 GHz	10 Gbps	OFDMA
802.15	2.4 GHz	2 Mbps	FHSS
802.16 (WiMAX)	10 to 66 GHz	120 Mbps	OFDM
802.20 (Mobile Wireless Access Working Group)	Below 3.5 GHz	1 Mbps	OFDM
Bluetooth	2.4 GHz	24 Mbps	Gaussian frequency shift keying (GFSK)
HiperLAN/2	5 GHz	54 Mbps	OFDM

Understanding Authentication

- Problem of unauthorized users accessing resources on a network
  - A major concern for security professionals
  - An organization that introduces wireless technology to the mix increases the potential for security problems

The 802.1X Standard

- Defines the process of authenticating and authorizing users on a network
- Basic concepts
  - Point-to-Point Protocol (PPP)
  - Extensible Authentication Protocol (EAP)
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Setup (WPS)

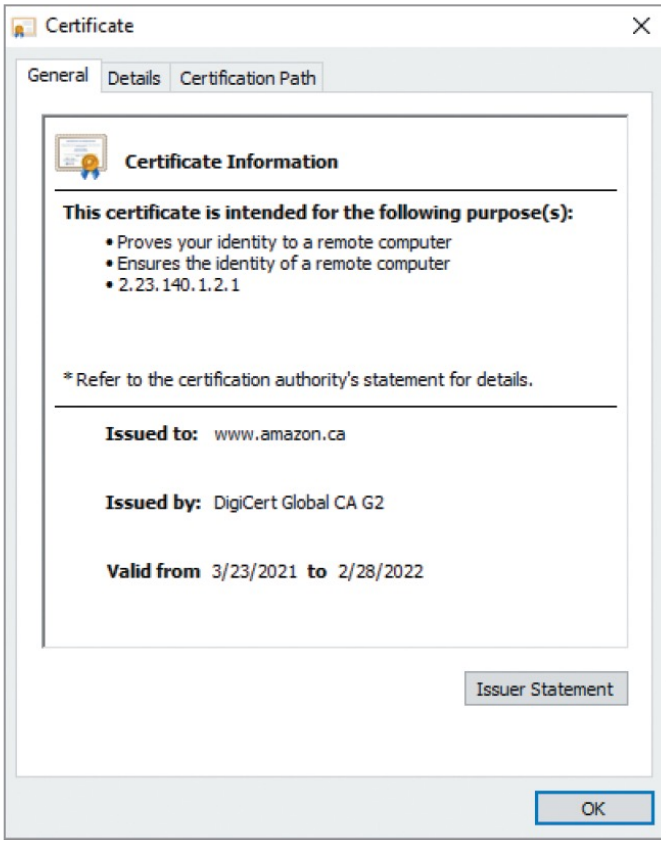
Point-to-Point Protocol (PPP)

- Many ISPs use PPP
  - To connect dial-up or DSL users
  - PPP handles authentication by requiring a user to enter a valid username and password
  - PPP verifies that users attempting to use the link are who they say they are

Extensible Authentication Protocol (EAP) (1 of 4)

- **EAP** is an enhancement to PPP
  - Designed to allow a company to select its authentication method
- Example:
  - A company can use certificates or Kerberos authentication to authenticate a user connecting to an AP
  - Certificate
    - Record that authenticates network entities, such as server or client
    - Contains X.509 information
      - Identifies the owner, the certificate authority (CA), and the owner's public key

Extensible Authentication Protocol (EAP) (2 of 4)



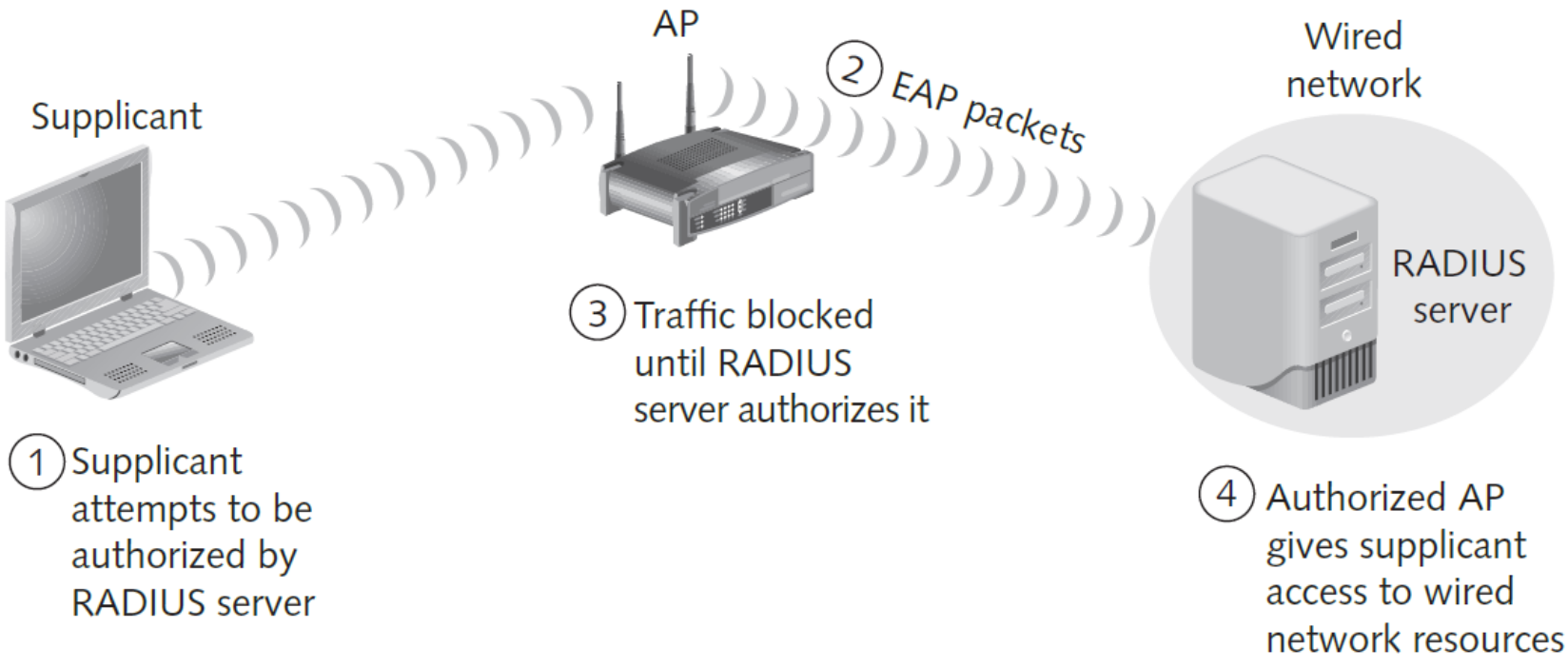
Source: Microsoft Windows

Figure 11-7 Viewing information about an x.509 certificate

Extensible Authentication Protocol (EAP) (3 of 4)

- EAP methods to improve security on wireless network:
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  - Protected EAP (P E A P)
  - Microsoft P E A P
- 802.1X uses the following components to function:
  - **Supplicant**
  - Authenticator
  - Authentication server

Extensible Authentication Protocol (EAP) (4 of 4)



Source: Cengage

Figure 11-8 A supplicant connecting to an AP and a RADIUS server

Wired Equivalent Privacy (WEP)

- Part of the 802.11b standard
- Developed to encrypt data traversing a wireless network
- WEP encryption is easily cracked
  - Due to a flaw in its RC4 encryption algorithm
- Works well for home users or small businesses when combined with the security of a Virtual Private Network (VPN)

Wi-Fi Protected Access (1 of 2)

- **WPA, WPA2, and WPA3**
  - Specified in the 802.11i standard
  - Replacement for WEP
- Improves encryption by using Temporal Key Integrity Protocol (TKIP) enhancements
  - TKIP's four enhancements that address encryption vulnerabilities in WEP
    - Message Integrity Check (M I C)
    - Extended Initialization Vector (IV) with sequencing rules
    - Per-packet key mixing
    - Rekeying mechanism
    - Authentication mechanism using 802.1X and EAP

Wi-Fi Protected Access (2 of 2)

- **WPA3**
  - Released in January 2018
  - Officially replaces WPA2 and provides improved security features
  - For encryption:
    - Uses AES-256 and SHA-384 in WPA3-Enterprise mode
    - Mandates the use of CCMP-128 (AES-128 in CCM Mode) as the minimum encryption algorithm in WPA3-Personal mode
    - Uses Simultaneous Authentication of Equals (SAE) exchange
      - Results in a more secure initial key exchange
  - Difficult for hackers to tap into a network using offline password-guessing attacks
  - Susceptible to timing attacks during the handshake process
    - Information gathered can be used for a password partitioning attack

Wi-Fi Protected Setup (WPS)

- **WPS**
  - A wireless authentication standard created to allow users to add devices easily and securely to a wireless network
  - Eliminates the need for a user to enter a passphrase
    - User simply presses a button on the router
    - The WPS-able device pairs with the router
- Flaw discovered in 2011
  - Allows an attacker to gain access to a network remotely without knowing the WPA2 password

Knowledge Check Activity 11-1

Which IEEE standard defines authentication and authorization in wireless networks?

a. 802.11
b. 802.11a
c. 802.11b
d. 802.1X

Knowledge Check Activity 11-1: Answer

Which IEEE standard defines authentication and authorization in wireless networks?

Answer: d. 802.1X

The 802.1X standard defines the process of authenticating and authorizing users on a network. This standard is especially useful for WLAN security when physical access control is more difficult to enforce than on wired LANs.

Polling Activity 11-1

Which wireless encryption standard offers the best security?

a. WPA3
b. WEP
c. WPS
d. WPA

Polling Activity 11-1: Answer

Which wireless encryption standard offers the best security?

Answer: a. WPA3

WPA3 makes it more difficult for hackers to tap into a network using offline password-guessing attacks. WPA2 would allow hackers to capture data from your router and use this data to repeatedly attempt to guess your password, but with WPA3, one incorrect hacking attempt renders this data useless. WPA3 also improves security over public Wi-Fi networks.

Knowledge Check Activity 11-2

What protocol was added to 802.11i to address WEP's encryption vulnerability?

a. MIC
b. TKIP
c. TTL
d. EAP-TLS

Knowledge Check Activity 11-2: Answer

What protocol was added to 802.11i to address WEP's encryption vulnerability?

Answer: b. TKIP

Temporal Key Integrity Protocol (TKIP) was added to the 802.11i standard as WEP was known to have cryptographic weaknesses. WEP was replaced by Wi-Fi Protected Access (WPA).

Understanding Wardriving

- Hackers use **wardriving**
  - Driving around with inexpensive hardware and software that enables them to detect unsecured APs
- Wardriving is not illegal
  - But using the network resources discovered with wardriving is illegal

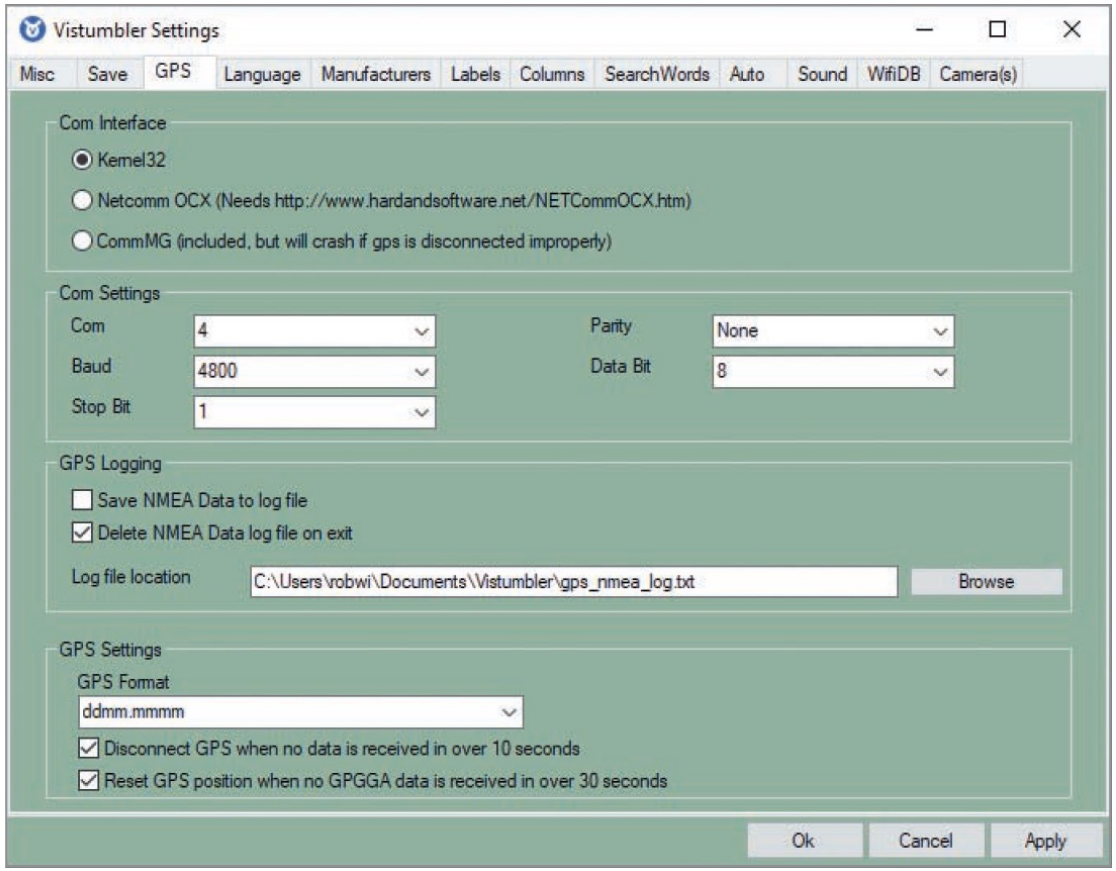
How It Works

- An attacker or security tester drives around with the following equipment:
  - A Wi-Fi capable smartphone or laptop and software that scans the areas for SSIDs
  - WNIC
    - Not all are compatible with scanning software
      - Review the software requirements before purchasing the hardware
- Antenna prices vary depending on the quality and the range that they can cover
- Most scanning software identifies:
  - The company's SSID
  - The security type enabled
  - The signal strength

Vistumbler (1 of 3)

- Freeware tool written for Windows that enables WLAN detection using certain access points
  - 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac
- Easy to install
- Primarily designed to assist security testers in the following:
  - Verify WLAN configuration
  - Detect other wireless networks that might be interfering with a WLAN
  - Detect unauthorized APs that might have been placed on a WLAN
- Capable of connecting to a GPS
  - Enables a security tester or hacker to map locations of all WLANs the software detects

Vistumbler (2 of 3)



Source: GNU General Public License (GNU GPL)

Figure 11-9 Configuring GPS settings in the Vistumbler Settings dialog box

Vistumbler (3 of 3)

- When Vistumbler identifies an AP signal, it logs the following:
  - The SSID
  - The MAC address
  - The manufacturer of the AP
  - The channel on which the signal was heard
  - The signal strength
  - Whether encryption is enabled
- Attackers can detect APs within a 350-foot radius
  - With better antennas, they can locate APs a couple of miles away

Kismet (1 of 2)

- Product for conducting wardriving attacks
  - Written by Mike Kershaw
  - Runs on Linux, BSD UNIX, macOS, and Linux PDAs
- A sniffer and an intrusion detection system (IDS)
  - Can sniff 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax traffic
- Features:
  - Wireshark- and Tcpdump-compatible data logging
  - Compatible with AirSnort and AirCrack
  - Network IP range detection
  - Detection of hidden network SSIDs

Kismet (2 of 2)

- Features (continued):
  - Graphical mapping of networks
  - Client or server architecture that allows multiple clients to view a single Kismet server at the same time
  - Manufacturer and model identification of APs and clients
  - Detection of known default AP configurations
  - XML output
  - Supports for dozens of card types

Polling Activity 11-2

What information can be gathered by wardriving? (Choose all that apply.)

a. SSIDs of wireless networks
b. Whether encryption is enabled
c. Whether SSL is enabled
d. Signal strength

Polling Activity 11-2: Answer

What information can be gathered by wardriving?

Answer: a., b., and d. SSIDs of wireless networks, whether encryption is enabled, and signal strength

In wardriving, most scanning software detects the company's SSID, the type of security enabled, and the signal strength, indicating how close the access point (AP) is to the attacker.

Discussion Activity 11-1

Discuss Temporal Key Integrity Protocol and identify which TKIP enhancement addresses the WEP vulnerability of forging packets.

Discussion Activity 11-1: Answer

Discuss Temporal Key Integrity Protocol and identify which TKIP enhancement addresses the WEP vulnerability of forging packets.

Answer: Message Integrity Check (MIC)

Explanation: Temporal Key Integrity Protocol (TKIP) is used by Wi-Fi Protected Access (WPA) to improve encryption. TKIP has four enhancements that address vulnerabilities in WEP. The vulnerability of forging packets is addressed by the Message Integrity Check (MIC) enhancement. MIC, pronounced M-I-C and also called Michael, is a cryptographic message integrity code. Its main purpose is to prevent forgeries, which are packets that attackers create to look like legitimate packets.

Understanding Wireless Hacking

- Hacking a wireless network
  - Not much different from hacking a wired LAN
- Techniques
  - Port scanning
  - Enumeration tools

Tools of the Trade (1 of 4)

- Equipment:
  - Laptop computer
  - WNIC
  - Antenna
  - Sniffers
- Tools for cracking WEP or WPA keys:
  - Aircrack-ng

Tools of the Trade (2 of 4)

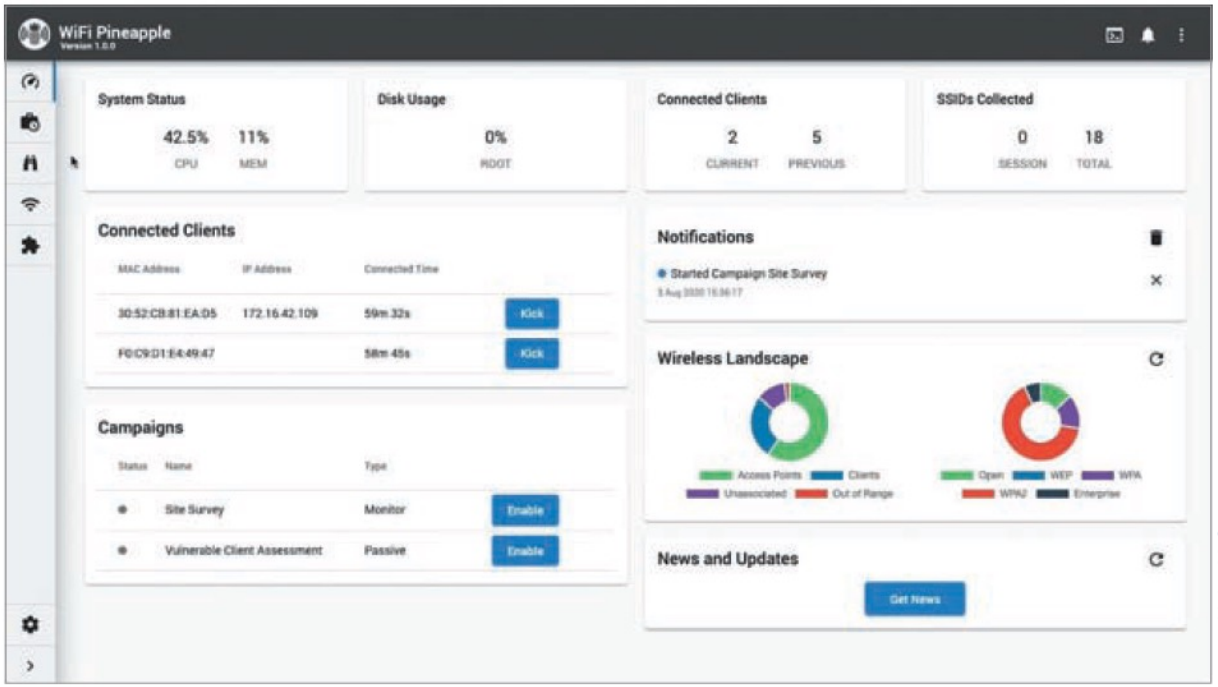
- Aircrack-ng
  - The tool most hackers use to access WEP-enabled WLANs
  - Replaced AirSnort
  - Has some useful add-ons
    - GUI front-end called Fern WIFI Cracker

Tools of the Trade (3 of 4)

Source: GNU General Public License (GNU GPL)

Figure 11-11 Fern WIFI Cracker interface

Tools of the Trade (4 of 4)



Source: Hak5 LLC

Figure 11-12 WiFi Pineapple interface

Countermeasures for Wireless Attacks (1 of 3)

- Consider using anti-wardriving software
  - Makes it more difficult for attackers to discover your WLAN
    - Honeypots
- Use measures for preventing radio waves from leaving or entering the building
  - Use a certain type of paint on the walls
- Use a router to only allow approved MAC addresses to access your network

Countermeasures for Wireless Attacks (2 of 3)

- Consider using an authentication server to authenticate users
  - Instead of relying on a wireless device
- Consider using EAP
  - Allows using different protocols that enhance security
- Consider placing the AP in the demilitarized zone (DMZ)
  - Use a firewall in front of the company's internal network that filters out traffic from unauthorized IP addresses
- If possible, upgrade to WPA2 or WPA3, and replace hardware that can't be upgraded

Countermeasures for Wireless Attacks (3 of 3)

- Assign static IP addresses to wireless clients
  - Instead of using DHCP
- Disable WPS
  - Removes the known WPS attack vectors
- Change the default SSID and disable SSID broadcasts
  - If you can’t disable SSID broadcasts, rename default SSID

Self-Assessment

What are the different types of attacks that an enterprise faces today?

What are the threats and vulnerabilities associated with embedded and specialized devices and mobile devices?

Summary

- Now that the lesson has ended, you should be able to:
  - Explain wireless technology
  - Describe wireless networking standards
  - Describe the process of authentication
  - Describe wardriving
  - Describe wireless hacking and tools used by hackers and security professionals