CWNA Guide to Wireless LANs, Third Edition

Chapter 9: Wireless LAN Security Vulnerabilities

Objectives

- Define information security
- Describe the different types of wireless attacks
- List the legacy IEEE security protections
- Explain the vulnerabilities of wireless transmissions

Principles of Information Security

- The need to defend against many attacks on technology has created a new element of IT known as information security.

- Understanding basic principles of defense is an important first step in understanding WLAN security and its vulnerabilities.

What is Information Security?

- **Information security:** Task of securing digital information
  - Ensures protective measures properly implemented
  - Protects *confidentiality*, *integrity*, and *availability* (**CIA**) on the devices that store, manipulate, and transmit the information through products, people, and procedures

Challenges of Information Security

- Trends influencing increasing difficultly in information security:
  - Universally connected devices
  - Speed of attacks
  - Sophistication of attacks
  - Availability and simplicity of attack tools
  - Faster detection of vulnerabilities
  - Delays in patching
  - Distributed attacks
    - The "many against one" approach
  - User confusion

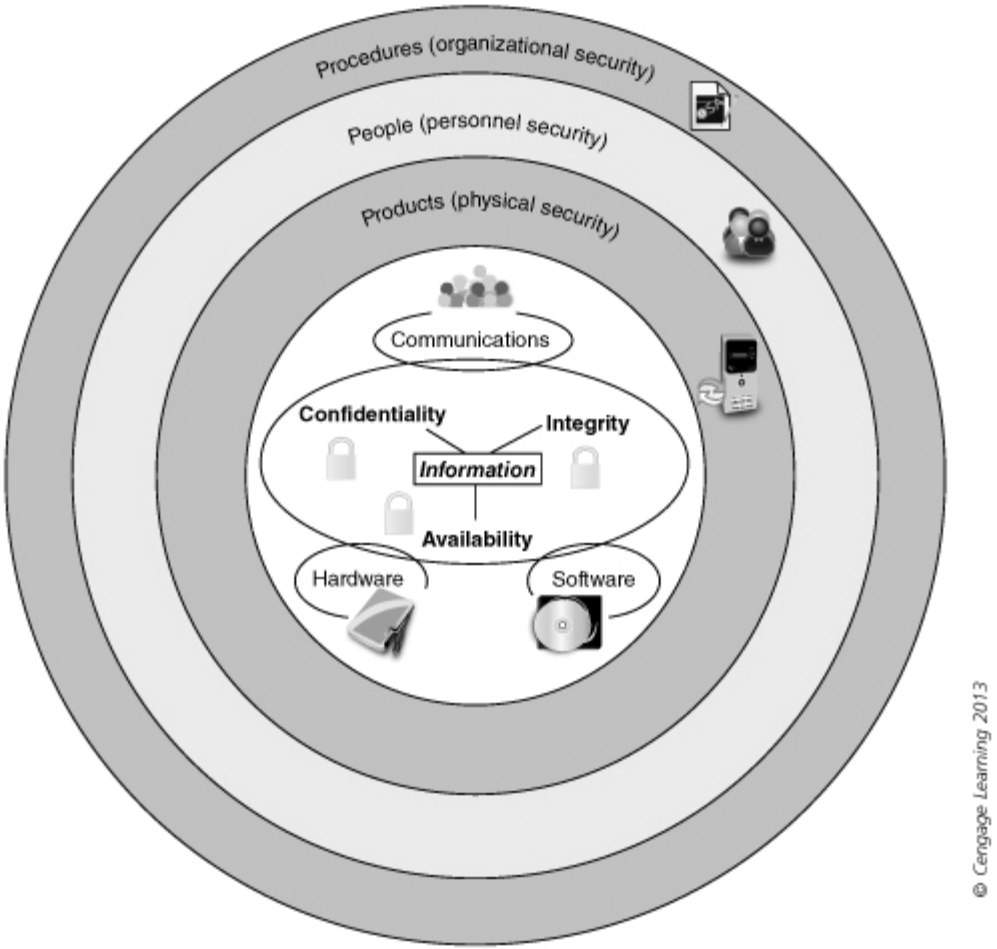

Figure 9-1 Information security components

Reason	Description
Universally connected devices	Attackers from anywhere in the world can send attacks.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes and hardware or software more quickly.
Delays in patching	Vendors are overwhelmed trying to keep pace by updating their products against attacks.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

Table 9-2 Difficulties in defending against attacks

Wireless Attacks

- Attacks can be divided into three categories:
  - Attacks against enterprise organizations
  - Attacks against mobile users
  - Attacks against home users

Enterprise Attacks

- **Attack Vectors**: paths that can be exploited
  - "*Hard edge*": well-defined boundary
  - Single entry point onto the network plus security devices that can defend it (firewall) make up a network's hard edge
  - Physical hard edge will help keep out unauthorized personnel so that attackers cannot physically access devices
  - Introduction of wireless LANs in enterprises has changed hard edges to "blurred edges"

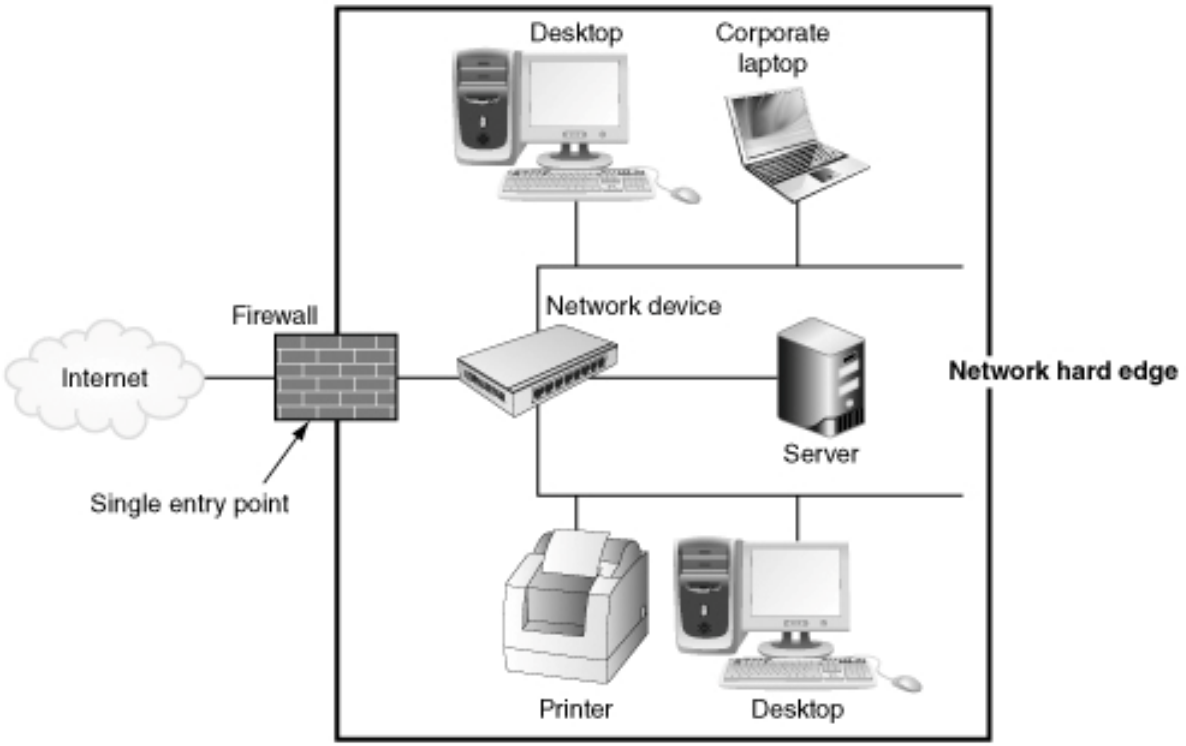

Figure 9-3 Network hard edge

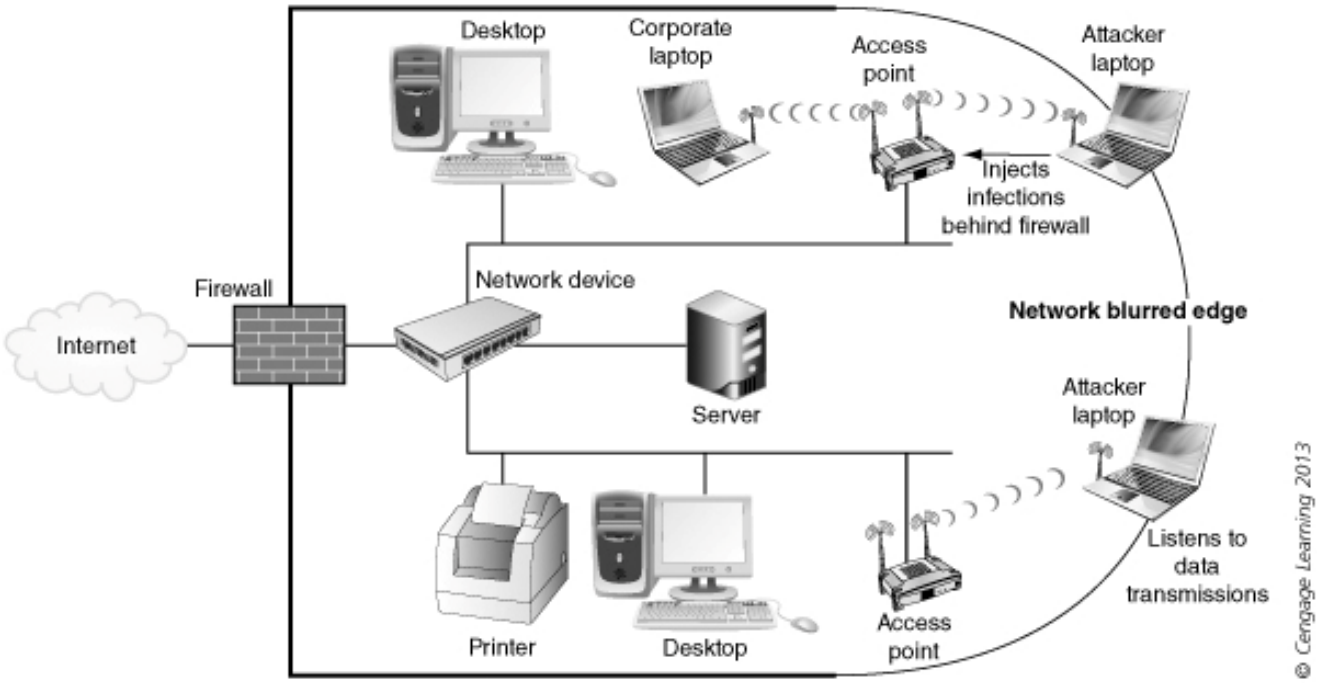

Figure 9-4 Network blurred edge

Enterprise Attacks

- A wireless device may create multiple enterprise attack vectors:
  - *Open or misconfigured AP*
  - *Rogue AP*: an employee may bring a device from home and connect it to the network
  - *Evil twin*: an AP that is set up by an attacker

Enterprise Attacks

- Wireless Enterprise Attacks:
  - **Reading Data**: attacker can pick up the RF signal from an open or misconfigured AP and read any confidential wireless transmissions and other traffic
  - **Hijacking Wireless Connections**: an attacker can trick a corporate mobile device to connect the imposter device instead
    - **Man-in-the-middle** attack: makes it appear that the wireless device and the network computers are communicating with each other, when actually they are sending and receiving data with an evil twin AP between them

Enterprise Attacks

- Wireless Enterprise Attacks (continued):
  - **Inserting Network Traffic**: injecting wireless packets into a network in order to redirect traffic to an attacker's server
  - **Denial of Service (DoS)**: attempts to prevent a device from performing its normal functions
    - An attacker can flood network with RF signal noise (called **RF jamming**)
    - An attacker can create a fictitious frame that pretends to come from a trusted client
    - Manipulating duration field values to a high number thus preventing other devices from transmitting for a long period of time

Mobile User Attacks

Typical Location	Attacker's Tool	Attack Description	User's Concern
Hotel	Wireless protocol analyzer	Read unencrypted transmissions from user's device to hotel AP	What confidential information could an attacker read from my wireless transmissions?
Airport	Laptop with wireless network interface adapter card	Set up an ad-hoc connection in a laptop so that a user connects directly to attacker's computer	Am I connected to a legitimate AP or is this an ad-hoc network?
Coffee shop	Laptop with software-based wireless AP	Configures software-based evil twin	Is my device actually connected to the coffee shop's hotspot?
School campus	Access point	Install evil twin AP in open commons area	Is my laptop probing for WLANs that are not on my safe list?
Remote office	Laptop with wireless network interface adapter card	Read broadcast and multicast wired network traffic	Do I have wired and wireless connections operating simultaneously?

Table 9-3 Mobile user attacks

Home Attacks

- Attacks against home WLANs are usually easy
  - Most home users fail to configure any security
- Attackers can:
  - *Steal data*
  - *Read wireless transmissions*: usernames, passwords, credit card numbers
  - *Inject malware*
  - *Download harmful content*
- **War driving**: searching for wireless signals from an automobile or on foot using a portable computer

Tool	Purpose
Mobile computing device	A mobile computing device with a wireless NIC can be used for war driving. This includes a standard portable computer, a pad computer, or a smartphone.
Wireless NIC adapter	Many war drivers prefer an external wireless NIC adapter that connects into a USB or other port and has an external antenna jack.
Antenna(s)	Although all wireless NIC adapters have embedded antennas, attaching an external antenna will significantly increase the ability to detect a wireless signal.
Software	Client utilities and integrated operating system tools provide limited information about a discovered WLAN. Serious war drivers use more specialized software.
Global positioning system (GPS) receiver	Although this is not required, it does help to pinpoint the location more precisely if this information will be recorded or shared with others.

Table 9-4 War driving tools

Legacy 802.11 Security Protections

- IEEE implemented several protections in the original 1997 802.11 standard
- Three categories of WLAN protections:
  - Access control
  - Wired equivalent privacy (WEP)
  - Authentication

https://www.youtube.com/watch?v=DspgyuedICM

https://www.youtube.com/watch?v=-Q_WXeEf8Fw

Access Control

- **Access Control**: granting or denying approval to use specific resources
- Wireless access control**:** Limit user's admission to AP
- **Media Access Control (MAC) address filtering:** Based on a node's unique MAC address

Figure 9-6 MAC address

Access Control

- MAC address filtering considered to be a basic means of controlling access
- Restrictions can be implemented in one of two ways:
  - A specific device can be permitted or the device can be blocked

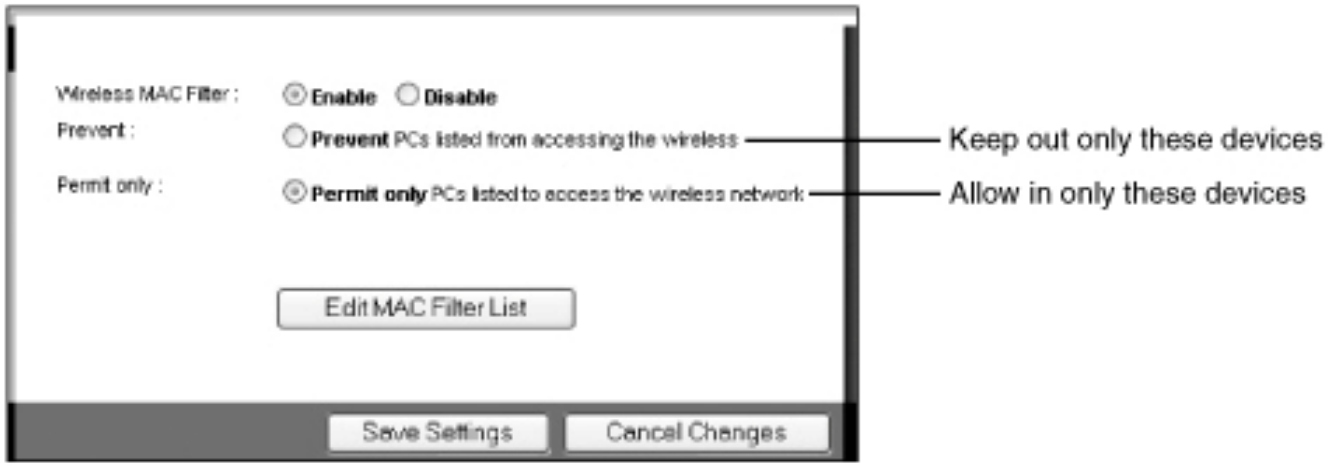

Figure 9-7 MAC address filtering

Wired Equivalent Privacy (WEP)

- Guard the confidentiality of information
  - Ensure only authorized parties can view it
- Used in IEEE 802.11 to encrypt wireless transmissions
  - "Scrambling"

Wired Equivalent Privacy (WEP)

- **Cryptography:** Science of transforming information so that it is secure while being transmitted or stored
  - "scrambles" data
- **Encryption:** Transforming **plaintext** to **ciphertext**
- **Decryption:** Transforming **ciphertext** to **plaintext**
- **Ciphertext:** Data that has been encrypted
  - Given a **key** that is used to encrypt and decrypt messages
  - **Weak keys:** Keys that are easily discovered

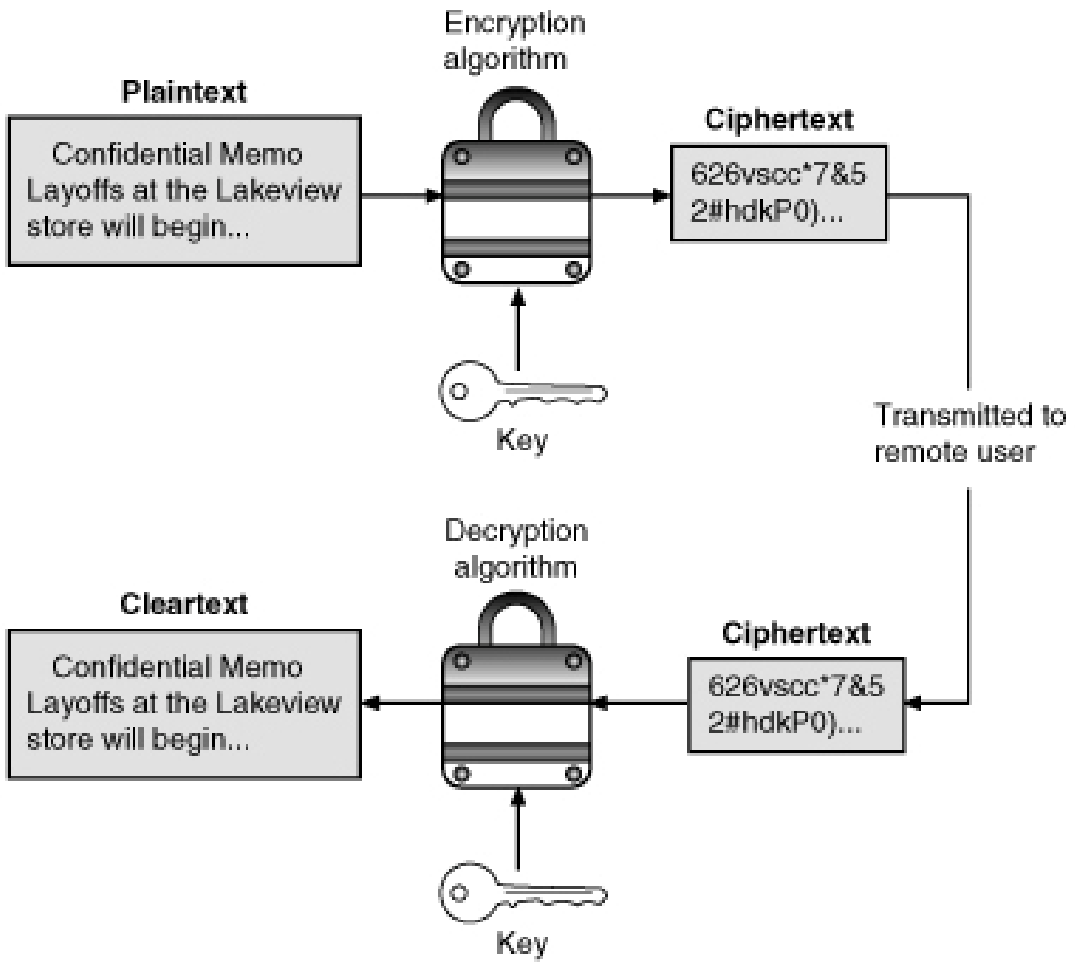

Figure 9-8 Cryptography process

Wired Equivalent Privacy (WEP)

- IEEE 802.11 cryptography objectives:
  - Efficient
  - Exportable
  - Optional
  - Reasonably strong
  - Self-synchronizing
- WEP relies on secret key "shared" between a wireless device and the AP
  - Same key installed on device and AP

Wired Equivalent Privacy (WEP)

- How WEP performs encryption:
  - Plaintext to be transmitted has Cyclic Redundancy Check (CRC) value that WEP calls this the **integrity check value (ICV)** – the CRC value is appended to the end of the text
  - Shared secret key is combined with an **initialization vector (IV)**
    - IV is a 24-bit value used in WEP that changes each time a packet is encrypted
  - Default key and IV are entered as the seed value into a **pseudo-random number generator (PRNG)** that creates a random number
    - Output is known as the **keystream**

Wired Equivalent Privacy (WEP)

- How WEP performs encryption (continued):
  - Text plus ICV and the keystream are combined to create encrypted text
  - The IV is added to the front of the ciphertext and the packet is ready for transmission

Wired Equivalent Privacy (WEP)

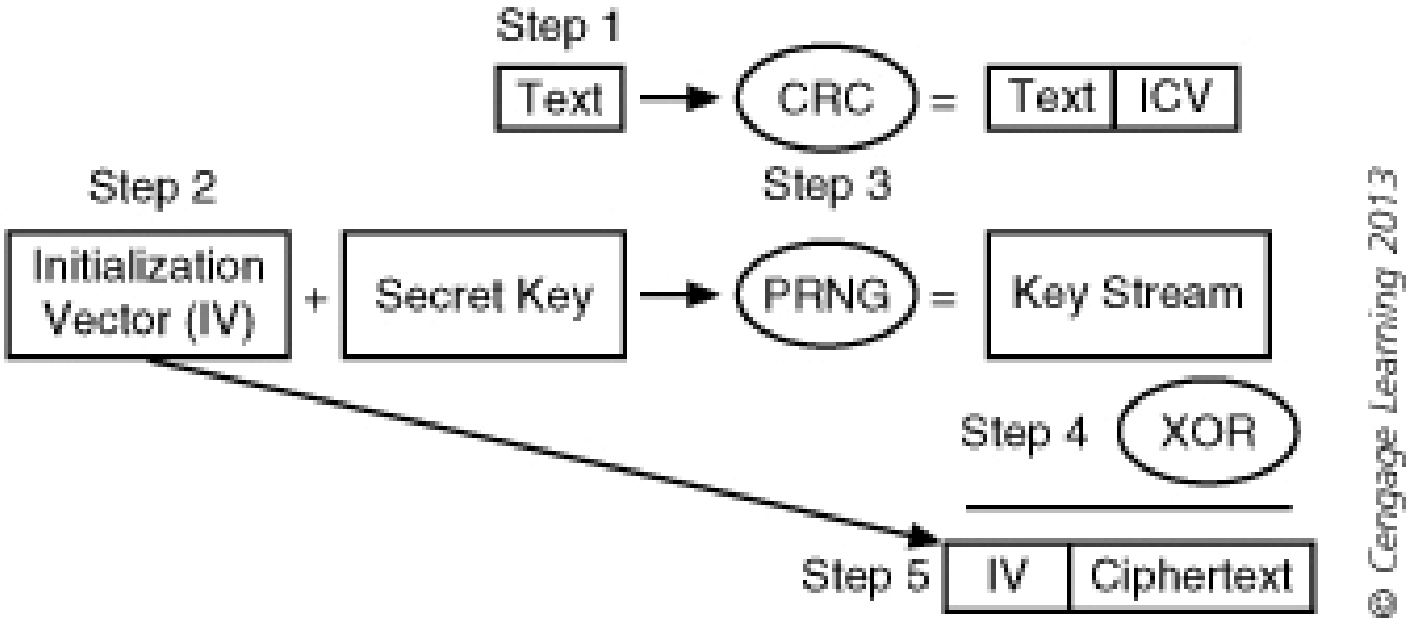

Figure 9-9 WEP encryption process

Wired Equivalent Privacy (WEP)

- When encrypted frame arrives at destination:
  - Receiving device separates IV from ciphertext
  - Combines IV with appropriate secret key
    - Create a **keystream**
  - Keystream used to extract text and ICV
  - Text run through CRC
    - Ensure ICVs match and nothing lost in transmission

Authentication

- **IEEE 802.11 authentication:** Process in which AP accepts or rejects a wireless device

- **Open system authentication:**
  - Wireless device sends association request frame to AP
    - Carries info about supported data rates and service set identifier (SSID)
  - AP compares received SSID with the network SSID
    - If they match, wireless device authenticated

Authentication

- **Shared key authentication:** Uses WEP keys
  - AP sends the wireless device the **challenge text**
  - Wireless device encrypts challenge text with its WEP key and returns it to the AP
  - AP decrypts returned result and compares to original challenge text
    - If they match, device accepted into network

Vulnerabilities of IEEE 802.11 Security

- IEEE 802.11 standard's security mechanisms for wireless networks have fallen short of their goal

- Vulnerabilities exist in:
  - Authentication
  - Address filtering
  - WEP

Authentication

- Inherently weak
  - Based only on match of SSIDs
  - SSID beaconed from AP during passive scanning
    - Easy to discover
- Some users configure their APs to prevent the beacon frame from including the SSID (known as **SSID hiding**)
- Limitations of SSID hiding:
  - SSID can still be discovered through management frames sent by the AP

Authentication

- Limitations of SSID hiding (continued):
  - SSID is initially transmitted in plaintext form when a device is negotiating with the AP
    - An attacker can force a renegotiation to discover SSID
  - SSID hiding may prevent users from roaming
  - Not all APs allow beaconing to be turned off
  - May cause connection problems with devices running Windows XP
  - SSID can be retrieved from an authenticated device
  - Many users do not change the default SSID, an attacker can try using default SSIDs

Authentication

- Shared key authentication, using challenge text, is also vulnerable
  - Attacker can view the key on an approved device by looking over someone's shoulder (called shoulder surfing)
  - AP send the challenge text to a devices as cleartext

Address Filtering

- MAC address filtering vulnerabilities:
  - Managing the number of MAC addresses in a medium to large sized wireless network can be challenging
  - MAC addresses are initially exchanged in cleartext
  - MAC addresses can be "spoofed" or substituted in two ways
    - Some wireless NICs allow for a substitute MAC address to be used
    - There are programs available that allow you to spoof a MAC address

WEP

- Uses 64-bit or 128-bit number which is made up of a 24-bit IV and either a 40-bit or 104-bit default key
  - Shorter keys easier to crack
- WEP implementation violates cardinal rule of cryptography
  - Creates detectable pattern for attackers
  - APs end up repeating Ivs
- *Collision:* Two packets derived from same IV
  - Attacker can use info from collisions to initiate a **keystream attack**

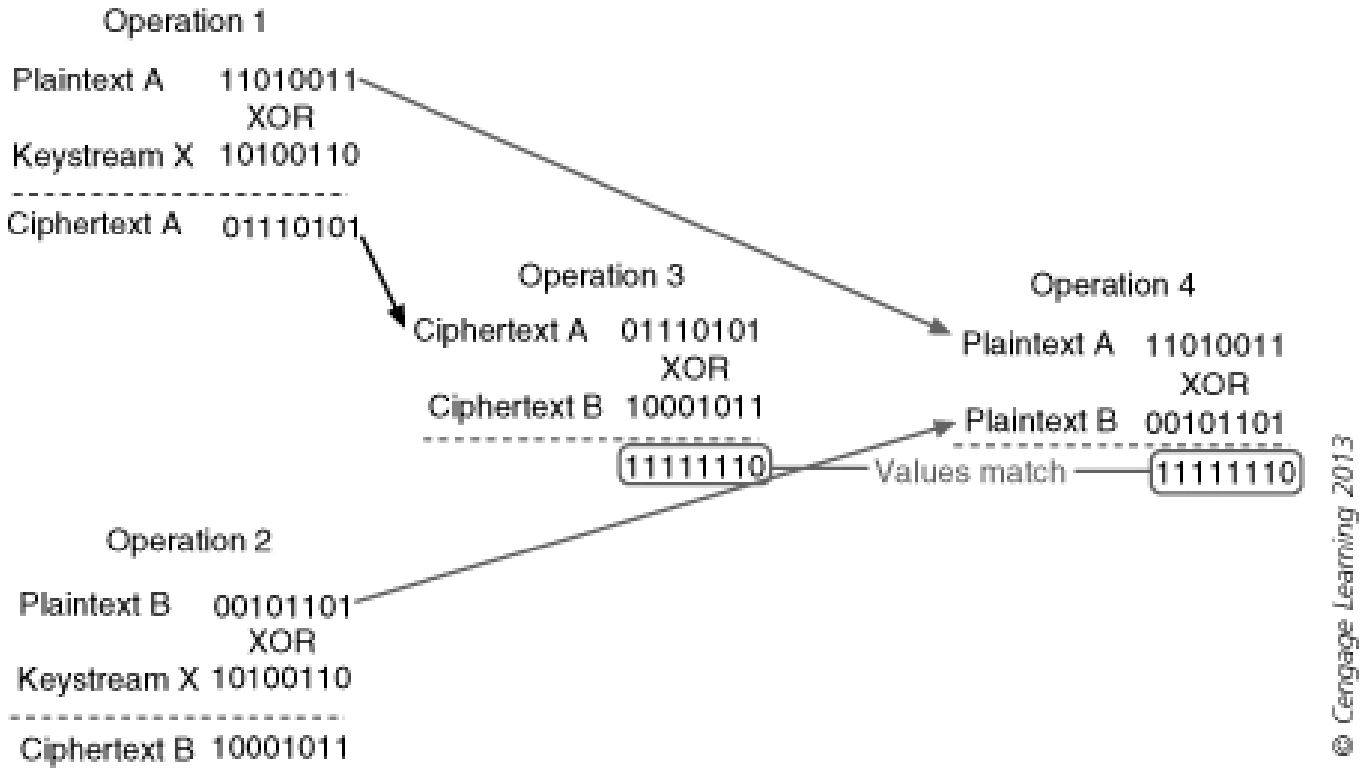

Figure 9-10 XOR operations

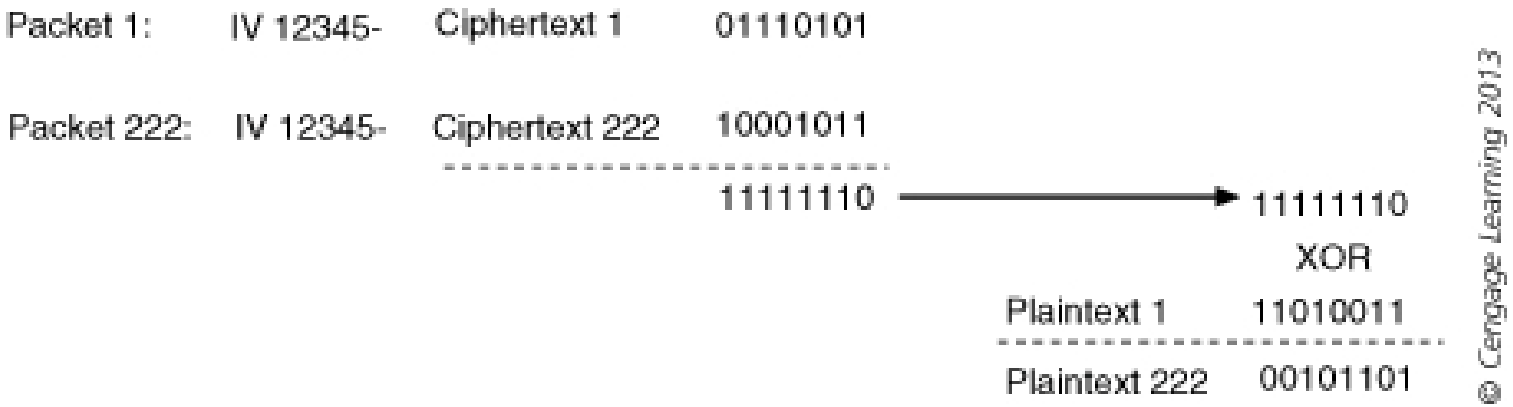

Figure 9-11 Capturing packets

WEP

- Several ways an attacker can use captured packets:
  - In fields where the value may not be known, the purpose is known so values can be guessed
  - Body portion of the text often encodes ASCII text, giving some possible clues
  - An attacker can capture an encrypted packed and based on its size may guess that it is an ARP request
    - Attacker can re-inject the ARP request into the network which will supply the attacker with many ARP responses

Summary

- Information security protects the confidentiality, integrity, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures
- Significant challenges in keeping wireless networks and devices secure
- There are multiple attack points in WLANS: open or misconfigured APs, rogue APs, and evil twins

Summary

- Attacks that can be launched include reading data, hijacking wireless connections, inserting traffic, and performing denial-of-service attacks
- Mobile users and home users face attacks as well
- IEEE implemented several protections in the original 802.11 standard: access control, wired equivalent privacy (WEP), and authentication
- Significant security vulnerabilities exist in the IEEE 802.11 security mechanisms