CWNA Guide to Wireless LANs, Third Edition

Chapter 10: Implementing Wireless LAN Security

Objectives

- Describe the transitional security solutions
- Describe the encryption and authentication features of IEEE 802.11i/WPA2
- List the features of wireless intrusion detection and wireless intrusion prevention systems
- Explain the features of wireless security tools

Transitional Solutions

- IEEE 802.11a and 802.11b standards included WEP specification
  - Vulnerabilities quickly realized
    - RC4 PRNG is not properly implemented
    - IV keys are reused
    - WEP does not prevent man-in-the-middle attacks
- IEEE and Wi-Fi Alliance started working on transitional solutions
  - WEP2, dynamic WEP, and Wi-Fi Protected Access (WPA)

WEP2

- Attempted to overcome WEP limitations by adding two new security enhancements
  - WEP key increased to 128 bits
  - **Kerberos** authentication
    - User issued "ticket" by Kerberos server
    - Presents ticket to network for a service
      - Used to authenticate user
- Soon was discovered that WEP2 had vulnerabilities
  - Collisions still occur
  - New dictionary-based attacks available

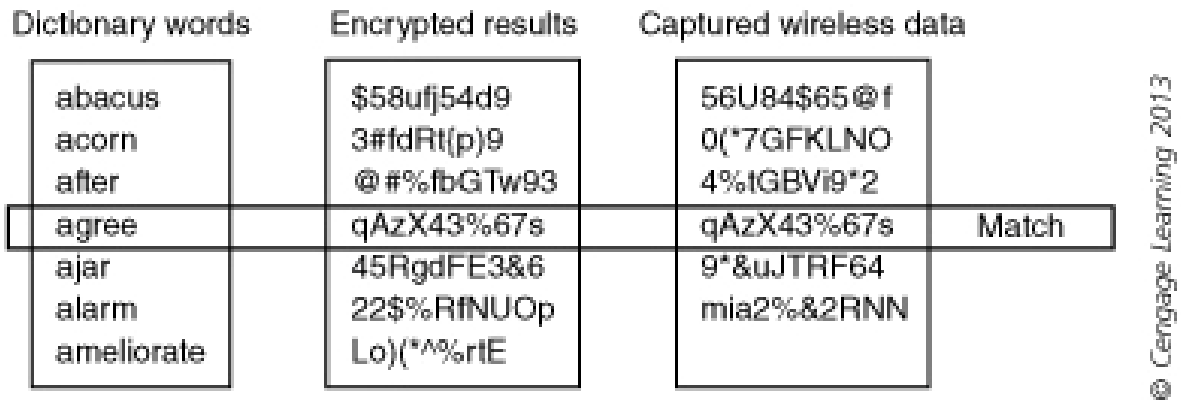

Figure 10-1 Dictionary attack

Dynamic WEP

- Solves weak IV problem by rotating keys frequently
  - More difficult to crack encrypted packet
- Uses different keys for **unicast** and **broadcast** traffic
  - Unicast WEP key unique to each user's session
    - Dynamically generated and changed frequently
  - Broadcast WEP key must be same for all users on a particular subnet and AP

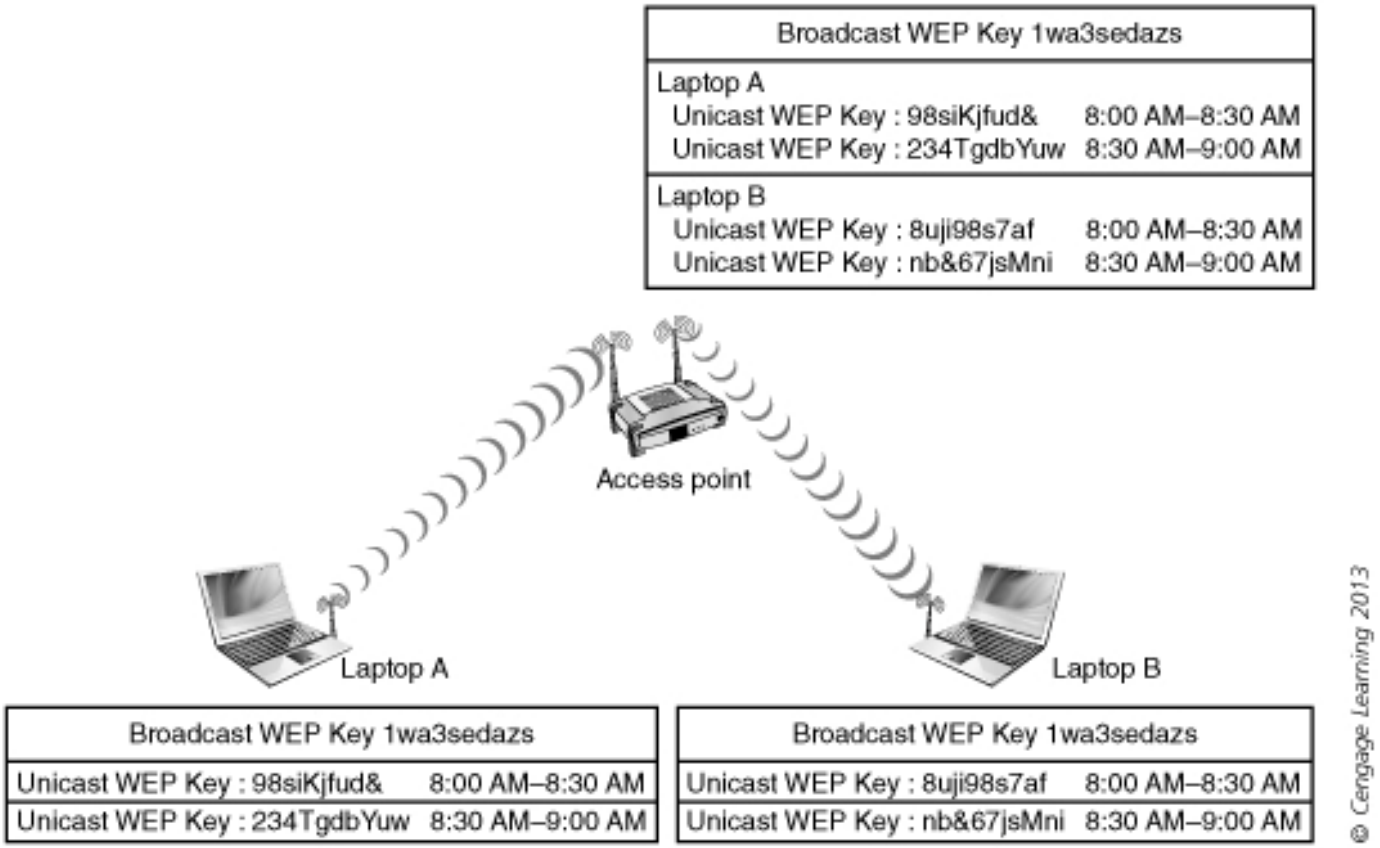

Figure 10-2 Dynamic WEP

Dynamic WEP

- Can be implemented without upgrading device drivers or AP firmware
  - No-cost and minimal effort to deploy
- Does not protect against man-in-the-middle attacks
- Susceptible to DoS attacks

Wi-Fi Protected Access (WPA)

- While the IEEE TG worked on the 802.11i standard, the Wi-Fi Alliance grew impatient and decided to come up with their own security standard
- Introduced by the Wi-Fi Alliance in October 2003
- Two modes of WPA
  - WPA Personal: designed for individuals or small office-home office settings
  - WPA Enterprise: intended for large enterprises, schools, and government agencies

Wi-Fi Protected Access (WPA)

- **Temporal Key Integrity Protocol (TKIP):** Replaces WEP's encryption key with 128-bit **per-packet key**
  - Dynamically generates new key for each packet
    - Prevents collisions
  - Authentication server can use 802.1x to produce unique master key for user sessions
  - Creates automated key hierarchy and management system

Wi-Fi Protected Access (WPA)

- **Message Integrity Check (MIC):** Designed to prevent attackers from capturing, altering, and resending data packets
  - Replaces CRC from WEP
  - CRC does not adequately protect data integrity
- TKIP has three major components:
  - MIC: protects against forgeries
  - IV sequence: TKIP reuses the WEP IV field as a sequence number for each packet
  - TKIP key mixing: substitutes a temporary key for the WEP base key
    - changes with each packet

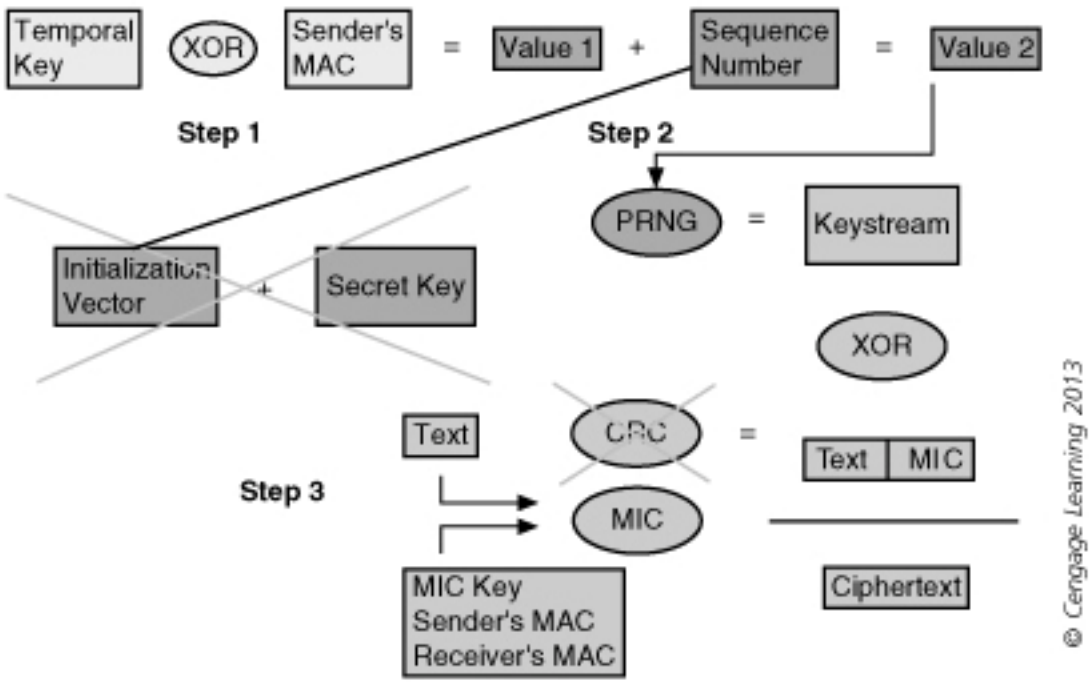

Figure 10-3 **TKIP encryption**, with WEP procedures that are not used with TKIP crossed out

Wi-Fi Protected Access (WPA)

- Authentication accomplished via IEEE 802.1x or **pre-shared key (PSK)** technology
  - PSK passphrase serves as **seed** for generating keys
- WPA weaknesses:
  - WPA was only designed as an interim, short-term solution to address critical WEP vulnerabilities

IEEE 802.11i/WPA2

- **IEEE 802.11i** was ratified in June 2004

- Provides solid wireless security model
  - **Robust security network (RSN)**

- **WPA2** was introduced in September 2004
  - Based on the final IEEE 802.11i standard
  - Almost identical to it
  - Two modes: WPA2 Personal and WPA2 Enterprise

- 802.11i/WPA2 addresses both encryption and authentication

Encryption

- Encryption accomplished by replacing RC4 **stream cipher** with a **block cipher**
  - Stream cipher: takes one character and replaces it with another character
  - Block cipher: manipulates entire block of plaintext at one time
- Block cipher used is **Advanced Encryption Standard (AES)**
  - Three step process
  - Second step consists of multiple **rounds** of encryption

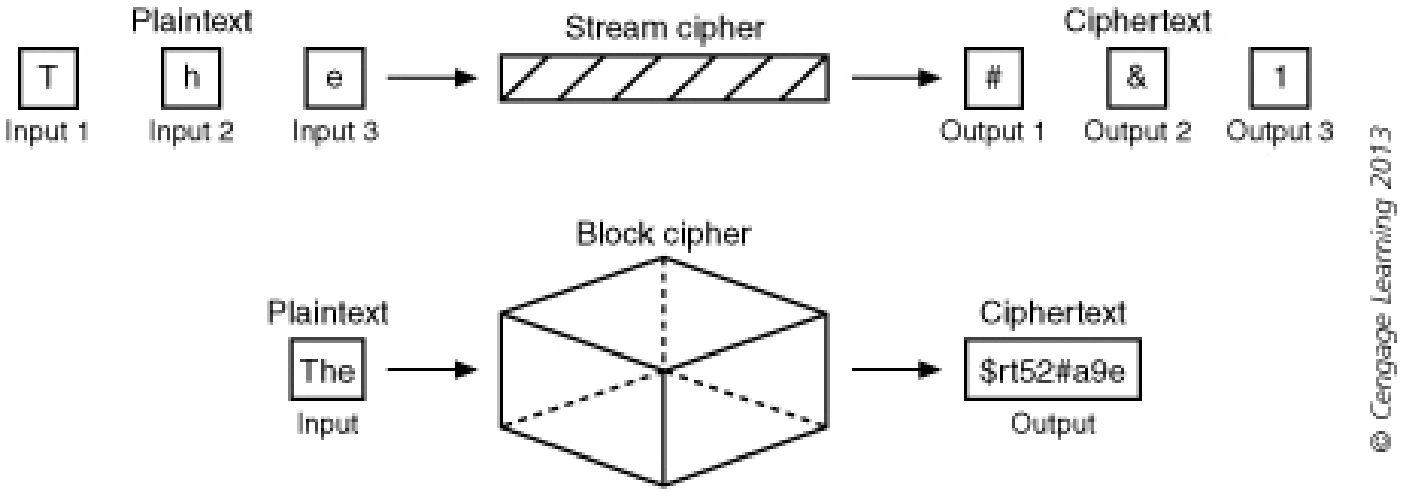

Figure 10-4 Stream cipher vs. block cipher

Encryption

- **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP):** Encryption protocol in 802.11i/WPA2
  - CCMP based on Counter Mode with CBC-MAC (CCM) of AES encryption algorithm
  - CCM provides data privacy
  - CBC-MAC provides data integrity and authentication
- CCMP and TKIP
  - Use 128-bit key for encryption
  - Includes a 48-bit value (called a packet number in CCMP)
  - Use a 64-bit MIC value

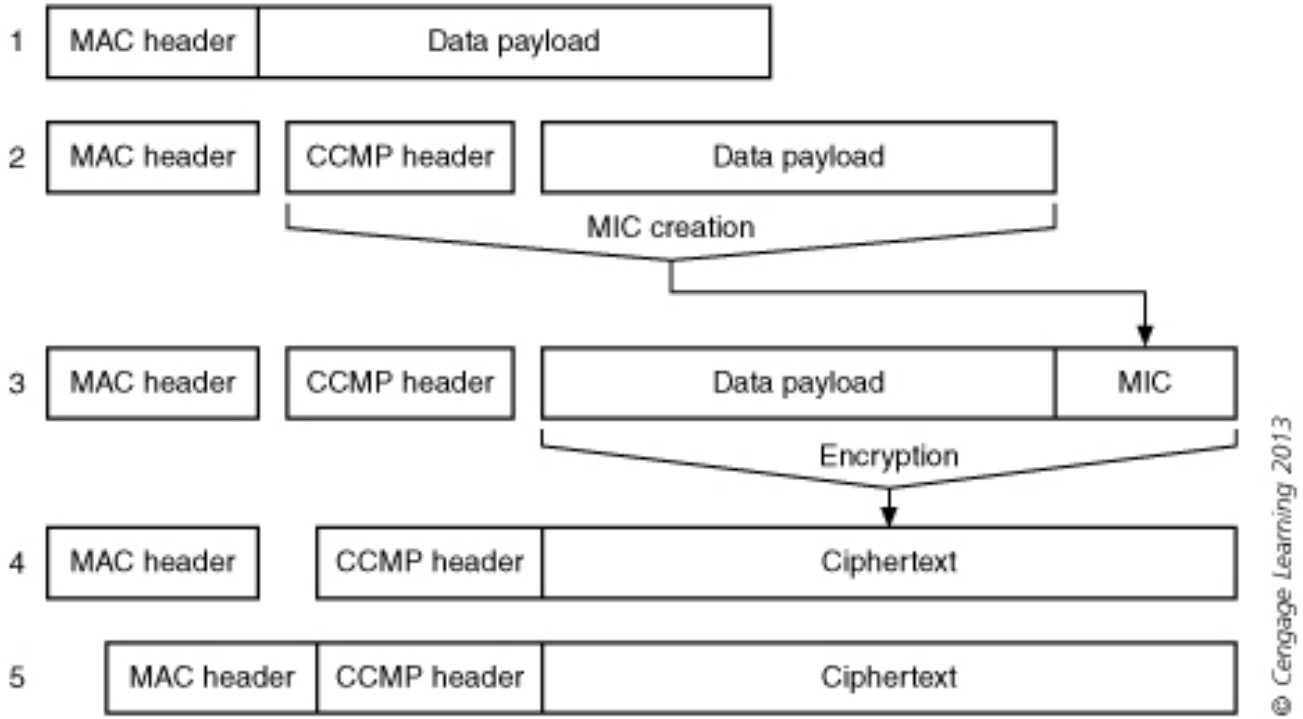

Figure 10-5 CCMP encryption process

Authentication

- IEEE 802.11i/WPA2 authentication and key management is accomplished by **IEEE 802.1X** standard
  - Implements **port security**
    - Blocks all traffic on port-by-port basis until client authenticated using credentials stored on authentication server
- 802.11X is often used in conjunction with **Remote Authentication Dial In User Service (RADIUS)**
  - Suitable for "high-volume service control applications"

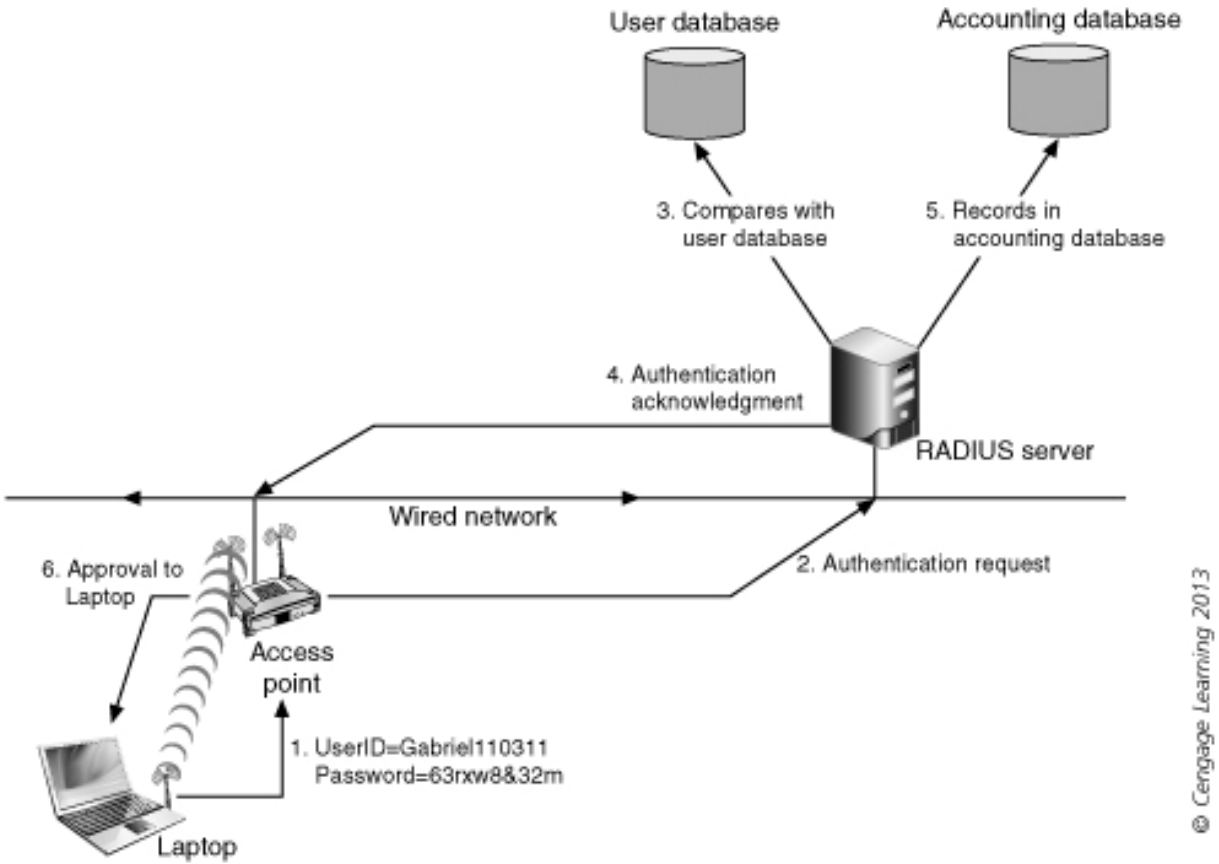

Figure 10-6 RADIUS authentication using IEEE 802.1X

Authentication

- **Extensible Authentication Protocol (EAP)**: framework for transporting the authentication protocols in an IEEE 802.1X network
  - There are seven different EAP protocols in WPA2 Enterprise
- **Per-User Preshared Keys (PPSK)**: combines many of the advantages of 802.1X with the ease of use of PSK
  - Unique passphrases can be assigned individually to each user while still using a common SSID

EAP Name	Description
EAP-TLS	An Internet Engineering Task Force (IETF) global standard protocol that uses digital certificates for authentication
EAP-TTLS/MSCHAPv2	This EAP protocol securely tunnels client password authentication within Transport Layer Security (TLS) records
PEAPv0/EAP-MSCHAPv2	This version of EAP uses password-based authentication
PEAPv1/EAP-GTC	PEAPv1 uses a changing token value for authentication
EAP-FAST	This EAP protocol securely tunnels any credential form for authentication (such as a password or a token) using TLS
EAP-SIM	EAP-SIM is based on the subscriber identity module (SIM) card installed in mobile phones and other devices that use Global System for Mobile Communications (GSM) networks
EAP-AKA	This EAP uses the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM) for authentication

Table 10-1 EAP protocols supported by WPA 2 Enterprise

Model	Category	Security Mechanism	Security Level
WPA2 Personal	Encryption	CCMP	High
WPA2 Personal	Authentication	PSK	Medium
WPA2 Enterprise	Encryption	CCMP	High
WPA2 Enterprise	Authentication	IEEE 802.1X	High

Table 10-2 WPA2 security models

Wireless Intrusion Detection and Prevention Systems

- **Intrusion system**: security management system that compiles information from a computer network or individual computer and then analyzes it to identify security vulnerabilities and attacks
  - Watches for systematic attacks instead of a single malicious packet
- Two types of intrusion systems for WLANs
  - Wireless intrusion detection system
  - Wireless intrusion prevention system

Wireless Intrusion Detection Systems (WIDS)

- **Wireless Intrusion Detection System (WIDS)**: constantly monitors the RF for attacks and sounds an alert if one is detected
- Different methods of detecting a wireless attack:
  - **Signature-based monitoring**: examining network traffic, activity, transactions, or behavior to compare against well-known patterns
  - **Anomaly-based monitoring**: detecting statistical anomalies
  - **Behavior-based monitoring**: using the normal processes and actions as standards

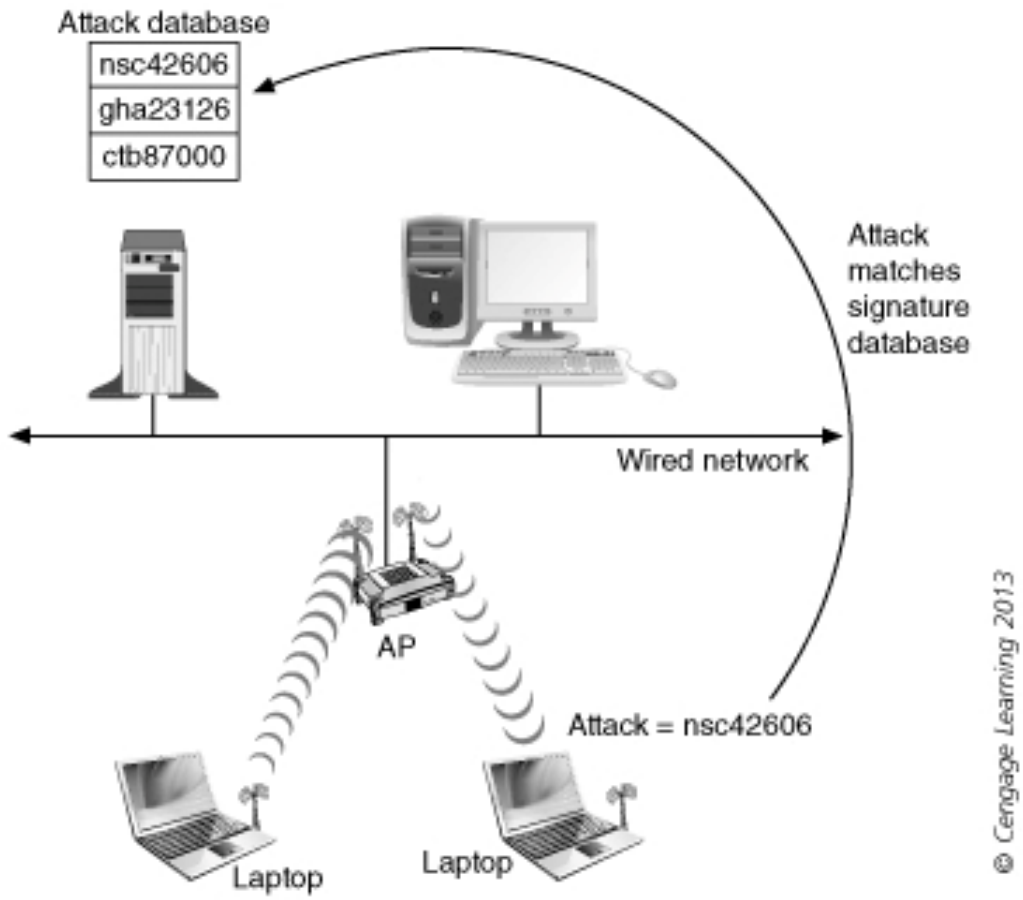

Figure 10-7 Signature-based WIDS

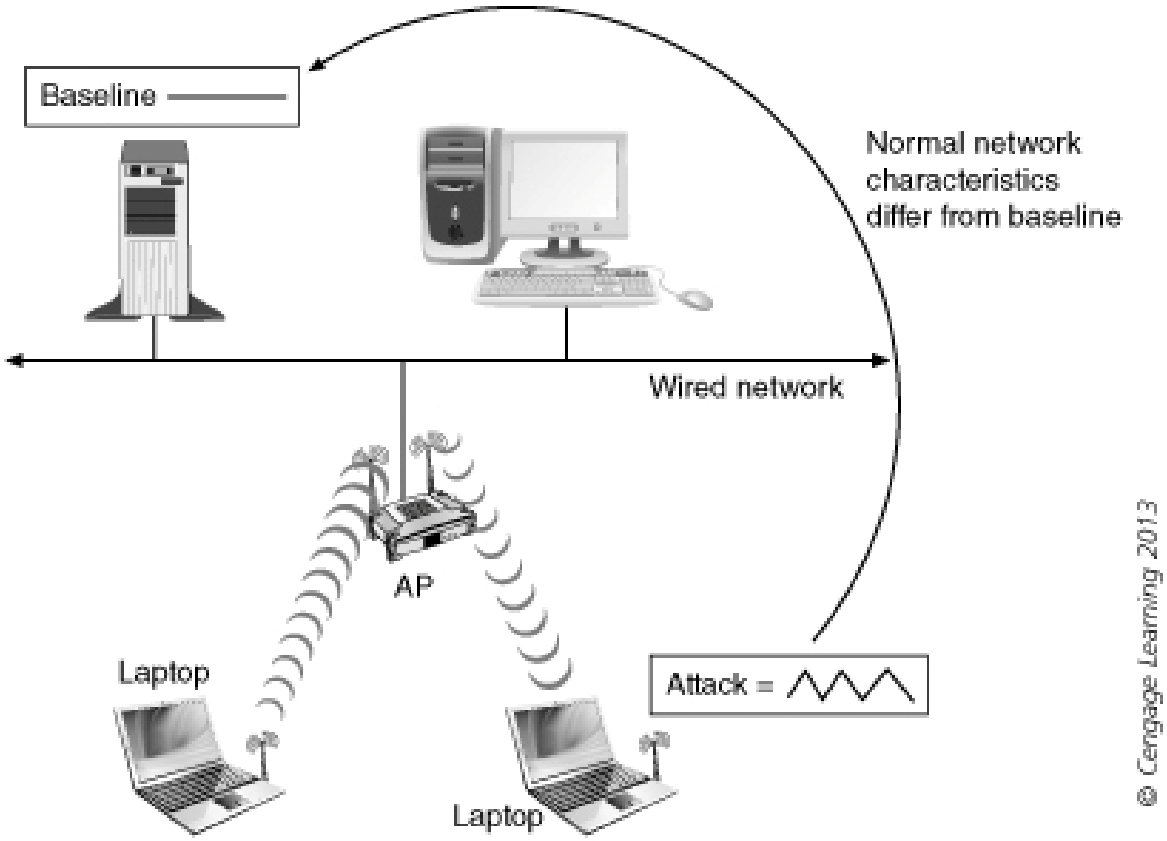

Figure 10-8 Anomaly-based WIDS

Wireless Intrusion Detection Systems (WIDS)

- Once a wireless attack is detected, a WIDS can perform different actions:
  - A *passive* WIDS will send information along (via e-mail or cell phone) and log the event
  - An *active* WIDS will send information along and take action
    - May configure firewall to filter out the IP address of the intruder
    - Launch a separate program to handle the event
    - Terminate the TCP session

Wireless Intrusion Prevention Systems (WIPS)

- Wireless intrusion prevention system (WIPS): monitors network traffic to immediately react to block a malicious attack
- Intended to improve upon the following disadvantages of WIDS:
  - WIDS cannot prevent an attack
  - WIDS only issues an alert after an attack has started
  - WIDS is dependent upon signatures
  - WIDS produces a high number of false positives

Wireless Intrusion Prevention Systems (WIPS)

- Major difference between WIDS and WIPS is location
  - A WIDS has sensors that monitor traffic entering and leaving a firewall and reports back to the central device for analysis
  - A WIPS could be located “in line” on the device itself
    - Allows the WIPS to more quickly take action to block an attack

WIDS/WIPS Sensors

- Both WIDS and WIPS rely upon sensors to monitor wireless network traffic and send summaries to a central analysis server for examination
- Two types of sensors
  - Integrated sensor (also called AP sensor or embedded sensor): uses existing APs to monitor the RF
    - Cost effective
  - Overlay sensor: uses dedicated sensors for scanning the RF for attacks
    - Can scan more frequencies provide broader coverage, and detect more attacks

Features

- **AP Identification and Categorization**
  - Ability to learn about the other APs that are in the area and classify those APs
    - Enables the WIDS/WIPS to recognize rogue APs without delay
  - APs are tagged as to their status:
    - *Authorized AP*: has been installed and configured by the organization
    - *Known AP*: foreign yet "friendly" AP
    - *Monitored AP*: signal is usually detected when scans are conducted
    - *Rogue AP*: does not fit the profile of the above three types

Features

- **Device Tracking**: involves the simultaneous tracking of all wireless devices within the WLAN
- Can be used for:
  - Asset tracking of wireless equipment that has a high value or have been stolen or misplaced (called **Real-Time Location Services** or **RTLS**)
  - Finding an emergency Voice Over Wi-Fi caller
  - Troubleshooting sources of wireless interference
  - Conducting a site survey
  - Determining a wireless user's availability status

Features

- **Event Action and Notification**: identifying and blocking any malicious activity
  - Once detected, security administrators must be notified through cell phones or e-mail alerts
- **RF Scanning**: All channels in the 2.4-GHz and 5-GHz range must be scanned
- **Protocol Analysis**: Several WIDS/WIPS products offer remote packet capture and decode capabilities

Attribute	Description
AP identification and categorization	All APs should detected and be automatically classified.
Device tracking	WIDS/WIPS must provide tracking of all wireless devices that are associated with the WLAN.
Event actions and notification	An attack must automatically be stopped and security personnel notified immediately.
RF scanning	The entire spectrum should be scanned by sensors.
Protocol analysis	An integrated protocol analyzer and decoder can reveal what is happening on the WLAN.

Table 10-3 Features of WIDS/WIPS

Other Wireless Security Tools

- Wireless security tools that can be used to protect a WLAN:
  - Virtual private network
  - Secure device management protocols
  - Wi-Fi Protected Setup
  - Role-based access control
  - Rogue AP discovery tools

Virtual Private Network (VPN)

- **Virtual private network (VPN):** Uses a public, unsecured network as if it were private, secured network
- Two common types:
  - *Remote-access VPN:* User-to-LAN connection used by remote users
  - *Site-to-site VPN:* Multiple sites can connect to other sites over Internet
- VPN transmissions are achieved through communicating with endpoints

Virtual Private Network

- *Endpoint:* End of tunnel between VPN devices
  - Can local software or a dedicated hardware device (such as a **VPN concentrator**)
- Software-based VPNs offer the most flexibility
  - Do not provide the same performance or security as a hardware-based VPN
- Hardware-based VPNs offer more features
  - Generally used for connecting two local area networks through the VPN tunnel

Secure Device Management Protocols

- **Secure Sockets Layer (SSL)**: protocol developed by Netscape for securely transmitting documents over the Internet
- **Transport Layer Security (TLS)**: protocol that guarantees privacy and data integrity between applications communicating over the Internet
- **Hypertext Transport Protocol over Secure Sockets Layer (HTTPS)**: secure version of HTTP
- **Secure Shell (SSH)**: an encrypted alternative to the Telnet protocol
  - Current version is SSH2

Secure Device Management Protocols

- **Simple Network Management Protocol (SNMP)**: allows network administrators to remotely monitor, manage, and configure devices on the network
  - SNMPv1 and SNMPv2 had several security vulnerabilities
  - SNMPv3 was introduced in 1998 and uses:
    - User names
    - Passwords
    - Encryption

Wi-Fi Protected Setup

- Wi-Fi Protected Setup (WPS): Optional means of configuring security on WLANs designed to help users who have little or no knowledge of security
- Two common WPS methods
  - PIN method: utilizes a Personal Identification Number (PIN) printed on a sticker of the wireless router or displayed through a software setup
  - Push-Button method: user pushes a button and the security configuration takes place

Role-Based Access Control (RBAC)

- Role-Based Access Control (RBAC): providing access based on a user's job function within an organization
  - RBAC model assigns permission to particular roles in the organization
  - Then assigns users to those roles

Rogue AP Discovery Tools

- A basic way to detect a rogue AP is to manually audit the airwaves using a protocol analyzer
- Most organizations elect to use a continual monitoring approach using a wireless probe
- Four types of wireless probes:
  - *Wireless device probe* (portable laptop computer)
  - *Desktop probe*
  - *AP probe*
  - *Dedicated probe*

Summary

- To address WEP vulnerabilities several transitional solutions were developed WEP2 and WPA
- WEP2 and WPA had their own security vulnerabilities
- The IEEE 802.11i and WPA2 standards provide a more solid wireless security model replacing the RC4 stream cipher with a more secure block cipher
- Encryption protocol used for both standards is CCMP with AES
- Authentication uses the 802.11X standard which is often used in conjunction with RADIUS

Summary

- A wireless intrusion detection system (WIDS) constantly monitors the RF for attacks
- Three methods for detecting a wireless attack: signature-based monitoring, anomaly-based monitoring, and behavior-based monitoring
- A wireless intrusion prevention system (WIPS) monitors network traffic to immediately react to block a malicious attack
- Both WIDS and WIPS rely on sensors to monitor wireless network traffic

Summary

- Additional security tools that can provide a high degree of security include virtual private networks, secure device management protocols, Wi-Fi Protected Setup, role-based access control, and rogue AP discovery tools