CWSP Guide to Wireless Security

Operational Support and Wireless Convergence

Objectives

- List the features of a secure and scalable wireless local area network
- Describe the functions of wireless operational support
- Explain WLAN, WiMAX, and 3G convergence

Features of a Scalable and Secure WLAN

- Scalable
  - Able to accommodate growth
- WLAN that has been designed from the outset to be secure and scalable
  - Will provide a solid foundation from which attacks can be thwarted and users can feel confident

Continuous Intrusion Monitoring and Containment

- One of the most important elements in a scalable and secure WLAN
- Monitoring a WLAN can be accomplished via:
  - A standard network management protocol
  - A system specifically designed for wireless networks
- Dedicated WLAN management systems
  - Use discovery tools to continuously monitor the RF for attacks

Continuous Intrusion Monitoring and Containment (continued)

- Other solutions for continuous monitoring of a WLAN
  - Wireless intrusion detection system (WIDS)
  - Wireless intrusion prevention system (WIPS)

Role-Based Access Control

- Wireless authentication
  - Verifies that the person requesting access to the network is who they claim to be
- Access control
  - Mechanism for limiting access to resources
    - Based on the users' identities and their membership in various groups
- Role-based access control
  - Easier to establish permissions based on job classification
  - Considered a major step in keeping a WLAN secure

Traffic Filtering

- Restricts network traffic based on specific criteria
- Basic types of filters
  - Address filtering
  - Data filtering
  - Protocol filtering
- APs can be configured to filter traffic
- Difficult for an attacker to circumvent

Strong Encryption

- At the heart of any secure WLAN is strong encryption
- WLAN encryption options
  - Wired equivalent privacy (WEP)
  - IEEE 802.11i
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2)
- A secure WLAN should use WPA2 for its encryption

Scalable Authentication

- Strong authentication that has the ability to grow
  - Another essential element in a secure and scalable WLAN
- WPA Enterprise and WPA2 Enterprise models
  - Utilize IEEE 802.1x port-based authentication
- RADIUS (Remote Authentication Dial-In User Service)
  - It has become the preferred scalable wireless authentication solution

Scalable Authentication (continued)

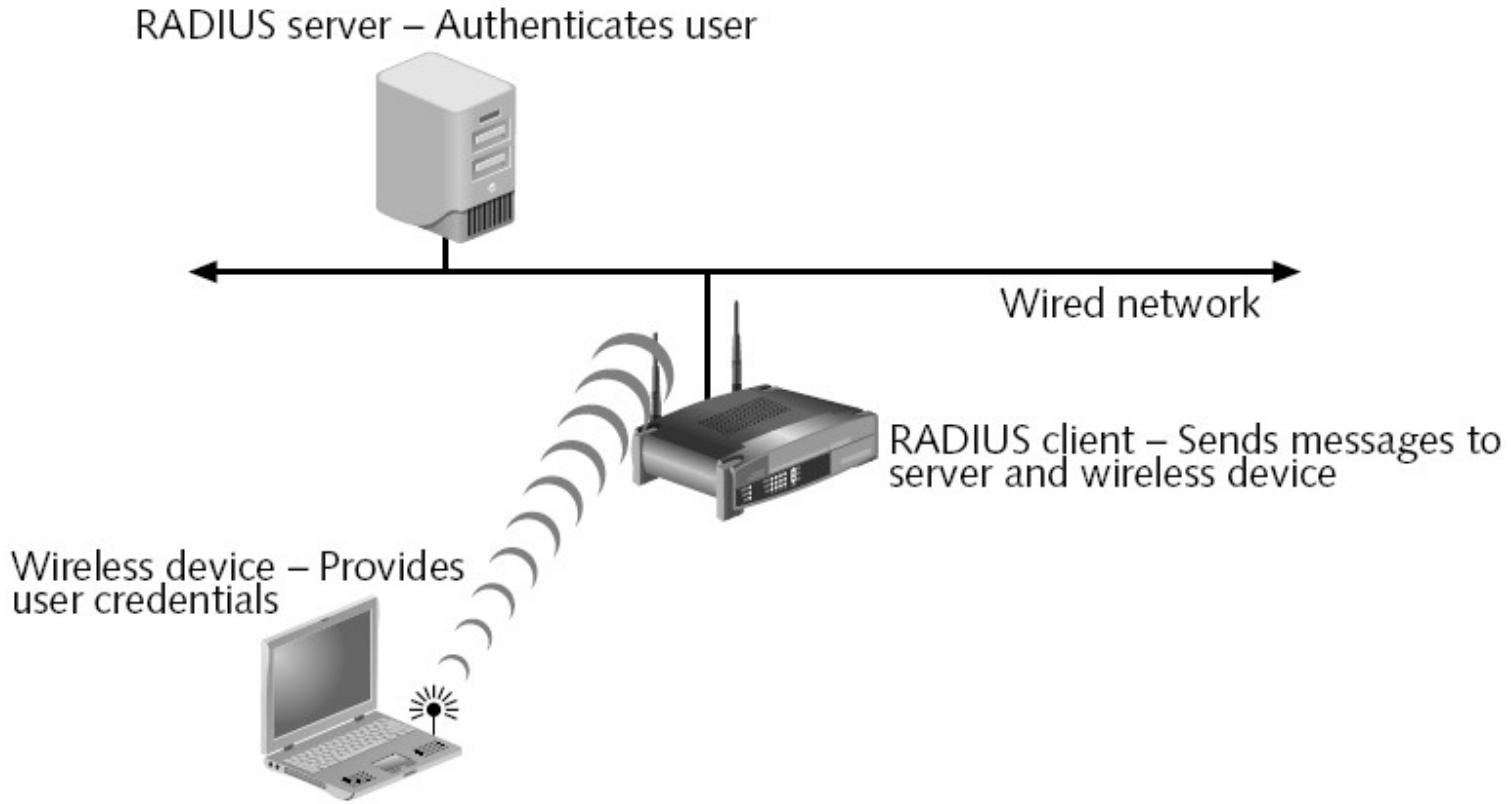

Figure 12-1 Wireless devices using RADIUS

Segmented Network Design

- Segmentation
  - Dividing the network into smaller units
- Wireless segmentation options
  - Wireless gateways
  - Wireless routers
  - Wireless switches
  - Firewalls
  - Demilitarized zones
  - Network address translation
  - Virtual local area network (VLAN)

Segmented Network Design (continued)

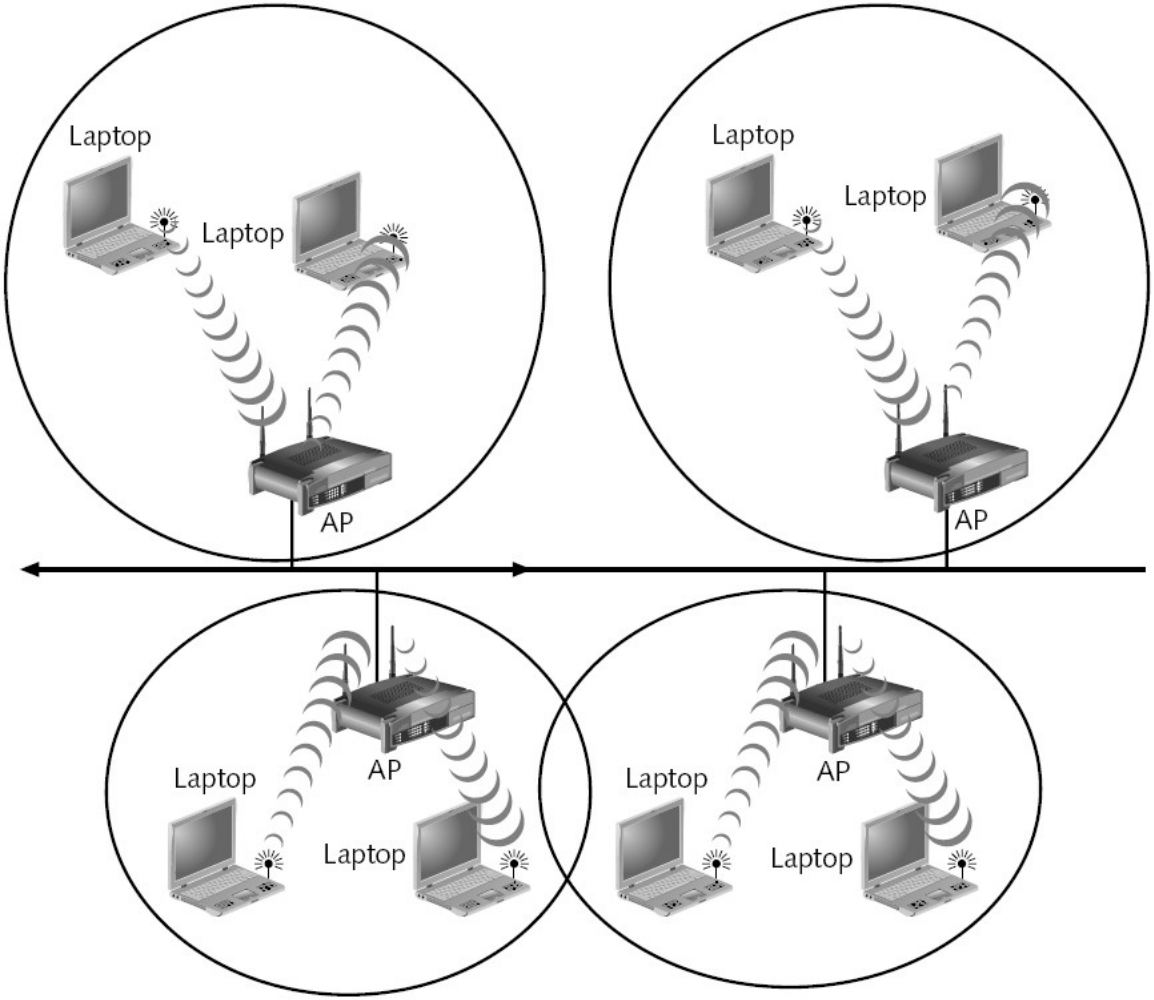

Figure 12-2 Wireless segmentation

Fast Handoff

- Original 802.11 standard
  - Did not specify how communications were to take place between APs
    - To support roaming users
- IEEE 802.11F
  - Specified information that access points need to exchange to support WLAN roaming
- IEEE 802.11r or fast handoff
  - Allows a wireless client to determine the quality of service (QoS) and security being used
    - At a different AP before making the transition

Fast Handoff (continued)

Table 12-1 Characteristics of a secure and stable WLAN

Technology	Benefit
Continuous intrusion monitoring and containment	Limits impact of attack
Role-based access control	Facilitates enforcing user permissions
Traffic filtering	Restricts attacks from entering network
Strong encryption	Prevents attacker from viewing transmissions
Scalable authentication	Provides strong authentication and easy to grow with organization
Segmented network design	Limits impact of attack
Fast handoff	Provides support for wider variety of applications

WLAN Operational Support

- No network functions on its own
- There must be operational support
  - To ensure its continued functionality and reliability
- Basic tasks
  - Monitoring
  - Configuration management
  - User training

Monitoring

- Monitoring tools for wired networks do not detect:
  - RF interference
  - Jamming
  - Location of APs
  - Identification of unauthorized users
- WLAN monitoring tools can be used to identify:
  - AP settings
  - Coverage
  - Network performance
  - Security audit

Configuration Management

- Controls changes made to WLAN after installation
- Types of changes
  - Applications
  - Coverage area
  - RF channel
  - Security
  - Transmit power
- Change request form
  - Outlines the requested alteration

Configuration Management (continued)

- WLAN baseline
  - Provides the standard for the operation of network
  - Used to evaluate how a proposed change may impact the WLAN
  - Typically includes a configuration management database
- Configuration management database
  - Listing of all installed wireless components, configuration settings, and diagrams
    - That document the current state of the wireless LAN

Education and Training

- Computer users share responsibility for protecting the assets of an organization
- Users need to receive training regarding:
  - Importance of securing information
  - Roles that they play in security
  - Necessary steps they need to take to ward off attacks
- Training must be ongoing
- User awareness is an essential element of security
- Organizations should provide education and training at set times and on an ad hoc basis

Education and Training (continued)

- Opportunities for education and training
  - A new employee is hired
  - A computer attack has occurred
  - An employee is promoted or given new responsibilities
  - A department is conducting an annual retreat
  - New user software is installed
  - User hardware is upgraded
- One challenge of security education and training
  - Understand how individuals learn

Education and Training (continued)

- How learners learn
  - Learning involves communication
  - Learning styles
    - Pedagogical approach
    - Andragogical approach
  - Adults learner types
    - Visual learners
    - Auditory learners
    - Kinesthetic learners (hands on)

Education and Training (continued)

Table 12-2 Pedagogical and andragogical traits

Subject	Pedagogical Approach	Andragogical Approach
Desire	Motivated by external pressures to get good grades or pass on to next grade	Motivated by higher self-esteem, more recognition, desire for better quality of life
Student	Dependent upon teacher for all learning	Student is self-directed and responsible for own learning
Subject matter	Defined by what the teacher wants to give	Learning is organized around situations in life or at work
Willingness to learn	Students are informed about what they must learn	A change triggers a readiness to learn or students perceive a gap between where they are and where they want to be

Education and Training (continued)

- Learning resources
  - An organization can provide educational content in several ways
    - Seminars and workshops
    - Print media
    - Internet information
      - Can be used in a daily basis

The Convergence of Wireless Technologies

- Convergence of wireless technology is most evident today in the blending of wireless LANs with wireless WANs
- Technologies supporting this unification besides WLAN
  - WiMAX, 4GLTE
  - Cellular 3G

WiMAX

- WiMAX (Worldwide Interoperability for Microwave Access)
  - Based on the IEEE 802.16 standard
- Fixed WiMAX
  - Officially IEEE 802.16-2004
  - Provides up to 50 kilometers (31 miles) of linear service range
    - And is not line-of-sight dependent
  - Provides shared data rates up to 70 Mbps

WiMAX (continued)

- Fixed WiMAX (continued)
  - Application categories
    - High-speed enterprise connectivity for business
    - Last mile connection
      - Connection that begins at a fast ISP and ends at the home or office
- Mobile WiMAX
  - Adds mobility components to Fixed WiMAX
  - Allows users to freely roam both indoors and outdoors for kilometers while remaining connected

WiMAX (continued)

- Mobile WiMAX (continued)
  - Competing standards
    - IEEE 802.16e
      - Extension of IEEE 802.16-2004
    - IEEE 802.20
      - Would permit users to roam up to 15 kilometers and at speeds up to 250 kilometers per hour

3G

- First Generation (1G)
  - Transmitted at 9.6 Kbps using analog circuit-switch technology
    - A dedicated and direct physical connection is made between the caller and the recipient
  - Can only be used for voice communications
- Second Generation (2G) – ie. EDGE
  - Used circuit-switched digital networks
  - Digital transmission advantages
    - Uses the frequency spectrum more efficiently
    - Quality of the voice transmission does not degrade

3G (continued)

- Second Generation (2G) (continued)
  - Digital transmission advantages (continued)
    - Difficult to decode and offers better security
    - Uses less transmitter power
    - Enables smaller and less expensive individual receivers and transmitters
- 2.5 Generation (2.5G)
  - Interim step between 2G and 3G
  - 2.5G networks operate at a max speed of 384 Kbps
  - 2.5G networks are packet-switched

3G (continued)

- 2.5 Generation (2.5G) (continued)
  - Ideal for voice communications
  - Not efficient for data transmission
  - Packet switching requires that the data transmission be broken into smaller units of packets
    - Each packet is sent independently through the network
  - Data transmissions occur in “bursts”
- Third Generation (3G)
  - Throughput rates for 3G averaging between 400 Kbps and 700 Kbps

3G (continued)

- Third Generation (3G) (continued)
  - Can be used for wireless data communications
- Mobile wireless data convergence
  - WLANs, WiMAX, and 3G may all be used together to provide wireless data services
  - WLAN hotspots continue to spread
  - Intel chipsets are available for laptop manufacturers
    - That incorporate WiMAX connectivity
  - “Road warriors” are installing combination 3G+WLAN PC Cards

3G (continued)

- Mobile wireless data convergence (continued)
  - VoWLAN types of security attacks
    - Attackers listening to voice conversations
    - User VoWLAN information captured and used to make free calls
    - Conversations corrupted by attackers
    - Denial of service attacks

Summary

- Designing and building a secure and scalable wireless LAN
  - Essential foundation for operational support of the network
- Operational support for a WLAN involves:
  - Monitoring
  - Configuration management
  - Education and training

Summary (continued)

- Different wireless technologies are converging to create a seamless wireless mobility experience for mobile users
- Technologies include:
  - WLAN
  - WiMAX
  - 3G

Quiz

1. True or False: SNMP allows computers and network equipment to gather data about network performance.

2. _____ restricts the traffic on a network based on specific criteria.

3. The WPA Enterprise and WPA2 Enterprise models utilize IEEE _____ port-based authentication.

4. A(n) _____ is a logical grouping of network devices within a larger network.

Quiz

1. A(n) _____ outlines the requested alteration in such a way that it can be determined what type of review is needed prior to accepting (or rejecting) the proposed changes.

2. The _____ refers to the connection that begins at a fast ISP, goes through the local neighborhood, and ends at the home or office.

3. The primary difference between 2G and 2.5G networks is that 2.5G networks are ____instead of circuit-switched.