Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

802.11: Infrastructure Reminder

- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - group of stations using the same AP
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS
Service Set Identifier - SSID

- Mechanism used to segment wireless networks
  - Multiple independent wireless networks can coexist in the same location
  - Effectively the name of the wireless network
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
  - AP can be configured to “broadcast” its SSID
  - Broadcasting can be disabled to improve security
  - SSID may be shared among users of the wireless segment

Association Management

- Stations must associate with an AP before they can use the wireless network
  - AP must know about them so it can forward packets
  - Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: finding out what access points are available
  2. Selection: deciding what AP (or ESS) to use
  3. Association: protocol to “sign up” with AP – involves exchange of parameters
  4. Authentication: needed to gain access to secure APs – many options possible
- Disassociation: station or AP can terminate association

Association Management: Scanning

- Stations can detect AP based by scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
  - Beacons are sent roughly 10 times per second
  - Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
  - Saves time – is more thorough
  - Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
  - Especially with passive scanning
  - Cannot transmit and receive frames during most of that time – not a big problem during initial association

Association Management: Selecting an AP and Joining

- Selecting a BSS or ESS typically must involve the user
  - What networks do you trust? Are you willing to pay?
  - Can be done automatically based on stated user preferences (e.g. the “automatic” list in Windows)
- The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm
  - Uses the information from the scan
  - Typically simply joins the AP with the strongest signal
- Associating with an AP
  - Synchronization in Timestamp Field and frequency
  - Adopt PHY parameters
  - Other parameters: BSSID, WEP, Beacon Period, etc.
Association Management: Roaming

- Reassociation: association is transferred from active AP to a new target AP
  - Supports mobility in the same ESS – layer 2 roaming
- Reassociation is initiated by wireless host based on vendor specific algorithms
  - Implemented using an Association Request Frame that is sent to the new AP
  - New AP accepts or rejects the request using an Association Response Frame
- Coordination between APs is defined in 802.11f
  - Allows forwarding of frames in multi-vendor networks
  - Inter-AP authentication and discovery typically coordinated using a RADIUS server
  - “Fast roaming” support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Association Management: Reassociation Algorithms

- Failure driven: only try to reassociate after connection to current AP is lost
  - Typically efficient for stationary clients since it not common that the best AP changes during a session
  - Mostly useful for nomadic clients
  - Can be very disruptive for mobile devices
- Proactive reassociation: periodically try to find an AP with a stronger signal
  - Tricky part: cannot communicate while scanning other channels
  - Trick: user power save mode to “hold” messages
  - Throughput during scanning is still affected though
    - Mostly affects latency sensitive applications

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11* QoS
WLAN Security Requirements

- Authentication: only allow authorized stations to associate with and use the AP
- Confidentiality: hide the contents of traffic from unauthorized parties
- Integrity: make sure traffic contents is not modified while in transit

Security in 802.11b

- WEP: Wired Equivalent Privacy
  - Achieve privacy similar to that on LAN through encryption
  - Intended to provide both privacy and integrity
  - RC4 and CRC32
  - Has known vulnerabilities
- WPA: Wi-Fi Protected Access
  - Larger, dynamically changed keys
- 802.1x: port-based authentication for LANs
  - Port-based authentication for LANs
- 802.11i (WPA2)
  - Builds on WPA
  - Uses AES for encryption

WLAN Security Exploits

- Insertion attacks
  - Unauthorized Clients or AP
- Client-to-Client Attacks
  - DOS - duplicate MAC or IP addresses
  - Can also be used to get free service on “secured” APs
- Interception and unauthorized monitoring
  - Packet Analysis by “sniffing” – listening to all traffic
- Jamming – denial of service
  - Cordless phones, baby monitors, leaky microwave oven, etc.

WLAN Security Exploits

- Brute Force Attacks Against AP Passwords
  - Dictionary Attacks Against SSID
- Encryption Attacks
  - Exploit known weaknesses of WEP
- Misconfigurations
  - APs ship in an unsecured configuration
  - Many people use APs with default configuration
MAC Filtering

- Each client identified by its 802.11 NIC Mac Address
- Each AP can be programmed with the set of MAC addresses it accepts
- Combine this filtering with the AP’s SSID
- Very simple solution
  » Some overhead to maintain list of MAC addresses
- But it is possible to forge MAC addresses …
  » Unauthorized client can “borrow” the MAC address of an authenticated client
  » Built in firewall will discard unexpected packets

Wired Equivalent Privacy

WEP

- Employs RC4 to Encrypt/Decrypt data
  » RC4 is a stream cypher based on a symmetric algorithm
  » 40 bit encryption key is supplied by the user
  » 24 bit initialization vector (IV) is supplied in the header
  » 64 bit string is seed for PRNG to generate a “key sequence”
  » 40 and 64 bit WEP are the same thing
- ICV (integrity check value) is computed for plaintext (CRC-32)
- ICV is appended to plaintext to create data string
- Key Sequence is XORéd to data string to create ciphertext
- Ciphertext and IV are sent to receiver
- 128-bit encryption uses a 104+24 bit key

WEP-Based Security Discussion

- WEP has known vulnerabilities
- Key can be cracked with a couple of hours of computing
  » IV transmitted in the clear
  » No protocol for encryption key distribution
  » Clever optimizations can reduce time to minutes
- All data then becomes vulnerable to interception
  » WEP typically uses a single shared key for all stations
- The CRC32 check is also vulnerable so that the data could be altered as well
  » Can makes changes without even decrypting!
- 128-bit WEP encryption is recommended

WEP Authentication

- Access request by client
- Challenge text sent to client by AP
- Challenge text encoded by client using shared secret then sent to AP
- If challenge text encoded properly, AP allows access; else access is denied
Port-based Authentication

- 802.1x is the IEEE standard for port-based authentication
- Users get a username/password to access the access point
- Was originally defined for switches but extended to APs
- Can be used to bootstrap other security mechanisms
  » Effectively creating a session

Wi-Fi Protected Access (WPA)

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
  » Uses a different Message Integrity Check
  » Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
  » Also frame counter in MIC to prevent replay attacks.
- Can be used with 802.1x authentication (optional)
  » It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
  » Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- 802.11i is a “permanent” security fix
  » Builds on the interim WPA standard (i.e. WPA2)
  » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
  » Better key management and data integrity
  » Uses 802.1x for authentication.

Wireless Security

- Security is not just about authentication and encryption
- Must also consider business and deployment issues
  » AAA: Authentication, Authorization, and Accounting
  » Supporting users at different levels

Authentication in WLAN Hotspots

- Upon association with the AP, only authentication traffic can pass through, as defined by IEEE 802.1x
- The protocol used to transport authentication traffic is the Extensible Authentication Protocol (EAP - RFC3748)
Dual SSID Approach

- VLAN1: Public
- VLAN2: Management
- VLAN3: User Traffic

- User traffic
- Authentication traffic
- Billing interface

- Access to DHCP server
- WPA/WEP encryption key

802.1x and EAP Protocol Execution

Best Practices for WiFi Security

- Use WPA2
  - Widely supported today
  - If not available, use WEP or WPA
    - Better than no security plus some possible legal benefits
- Change the default configuration of your AP:
  - Change default passwords on APs
  - Don’t name your AP by brand name
  - Don’t name your AP by model #
  - Change default SSID
- Use MAC filtering if available
- Use a VPN or application layer encryption
  - Must assume that wireless segment is untrusted
  - Provides end-to-end encryption – is what you want!

Wardriving

- The act of locating and possibly exploiting to a wireless network while driving around a city
- You need a vehicle, a laptop, a wireless PC card and some kind of antenna
- People can intercept your wireless signal when the signal exceeds your building
  - http://www.wardriving.com

- Is this legal??