CPE5021
Advanced Network Security

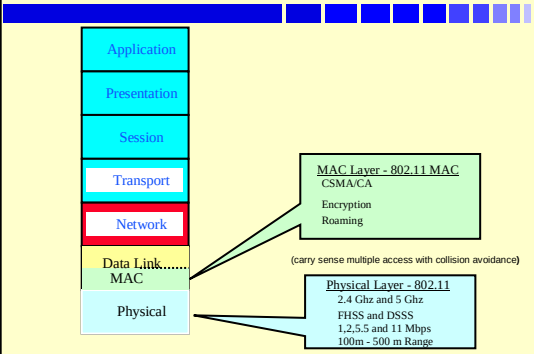
-- Wireless Network Security: Theory and Practice--

- Lecture 7

Wireless LAN Security Standard - 802.11a & 802.11b

- **IEEE 802.11b (Wi-Fi) Standard.**
  - Employs **Direct Sequence Spread Spectrum (DSSS)**
  - Operates in the 2.4 GHz band.
  - Has 14 channels (channels 1-14) spaced 5 MHz apart.
  - Supported data rates are 1, 2, 5.5, and 11 MBps.
- **IEEE 802.11a Standard.**
  - Employs **Orthogonal Frequency Division Multiplexing (OFDM)**.
  - Operates in the 5.0 GHz band.
  - Has 200 channels (channels 1-199) spaced 5 MHz apart.
  - Supported data rates are 6, 9, 12, 18, 24, 36, 48, and 54 MBps.
  - 6, 12, and 24 are mandatory. All others are optional.

802.11 Protocol Stack



Wireless Security

- **IEEE 802.15 Wireless Personal Area Network (WPAN)**
  - For short range and low power peripheral connections.
  - Employs FHSS (frequency-hopping spread spectrum) with TDMA (Time division multiple access) in the 2.4 Ghz ISM (Industrial, Scientific, and Medicine - frequency bands**)** band.
  - Short links from 30 - 300 feet.
  - Data rate up to 720 KBps
- **IEEE 802. 16 Wireless Metropolitan Area Network (WMAN)**
  - Intended for large area broadband wireless coverage
    - Becoming popular in US and UK.
  - Supports TCP/IP, VoIP and ATM services.
  - Security is based upon X.509 with RSA.
  - Operates in the range of 2Ghz - 66 Ghz.

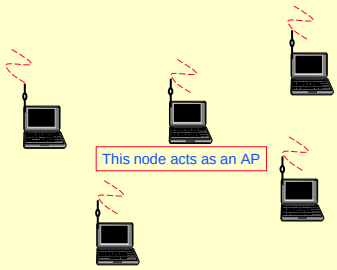
802.11 Basic Components

- **Wireless Medium.**
  - The Radio Frequency spectrum used to transfer frames between the wireless station and the AP or between wireless stations.
- **Wireless Stations.**
  - Computing devices with wireless network interfaces.
  - Typically battery operated laptops or handheld computers.
- **Access Points (AP).**
  - APs form a bridge between wired and wireless medium.
- **Distribution System (DS).**
  - A wired/wireless medium (with software) which connect APs to one another.

802.11 Topology
Independent Basic Service Set (IBSS).

- **Independent Basic Service Set**
  - **There is No** Access Point.
  - It is an **ad-hoc group** of wireless nodes.
  - Uses peer-to-peer transmission
  - One node is elected to act as a proxy to perform the functions of the AP.

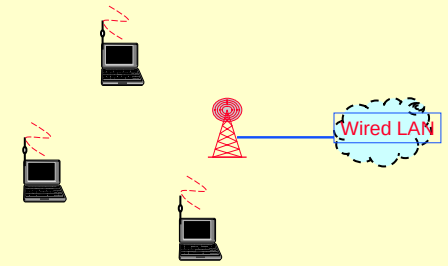
IBSS: example



802.11 Topology
Basic Service Set (BSS).

- **Basic Service Set**
  - A **single** Access Point
  - The AP acts as a **bridge** between wireless clients and the wired network.
  - **Roaming** is limited to a single radio cell
  - All clients operate on the same channel.
  - A BSS connected to a wired network is called an **Infrastructure BSS.**

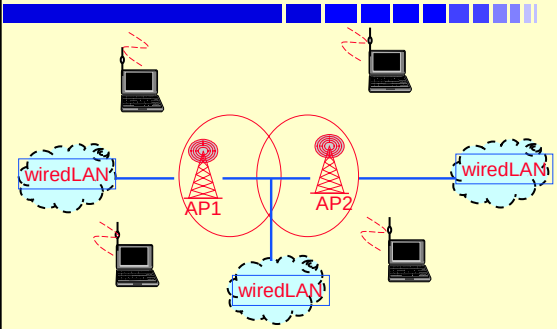
BSS: example



802.11 Topology
Extended Service Set (ESS).

- **Extended Service Set**
  - There are **Multiple Access Points** that communicate through the DS.
  - Each AP acts as a bridge between clients and the wired network.
  - Each AP is assigned a different channel and forms a radio cell.
  - All clients operate on the same channel in the same cell but can communicate through the DS.

ESS: example



802.11 Architecture
Network Services

- **Station Services**
  - **Authentication** - The client identifies itself to the AP in order to form an ***Association*** **by using**.
    - **Service Set Identifier (SSID), or**
    - **MAC Filtering**.
  - **De-authentication** - Destroys a previously known station identity- terminates the current association. It occurs when
    - The device shuts down.
    - The device is out of AP range.
  - **MAC Service Data Unit (MSDU) Data Delivery** - Reliable transfer of data from one MAC to another MAC.
    - **Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).**
    - **Request To Send/Clear To Send (RTS/CTS).**
  - **Privacy** - Confidentiality of the transmitted data.
    - E.g: **Wired Equivalency Protection (WEP)** with RC-4.

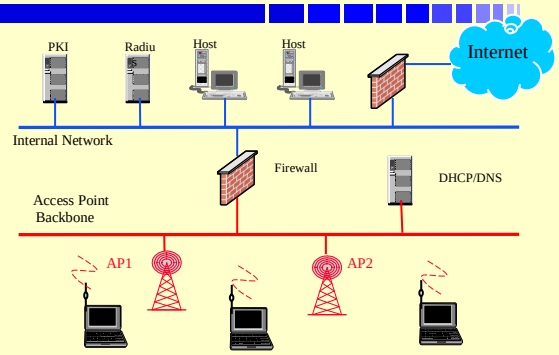
802.11 Architecture
Distribution (Systems) Services

- **Distribution Services.**
  - **Association** - establishes a logical connection between the client and the AP. i.e., a station registers with an AP.
    - Determines the location of the client for the DS.
    - Determines the path the DS needs to reach the client.
    - A client can be authenticated to multiple APs but Associated with only one AP.
  - **Reassociation** - Retains network session information when the wireless client passes from one AP to another AP.
    - This information tells the new AP the identify of the last AP.
    - This allows the old AP to forward any remaining frames to the new AP for delivery via the DS.

802.11 Architecture
Distribution Services

- **Disassociation** - Tears down the association between the AP and the wireless device.
  - The device leaves the AP area.
  - The AP is shutting down.
- **Distribution** - Determines the location to which a frame should be forwarded by the AP - An AP uses the DS to deliver frames.
  - Another AP.
  - A wireless client.
  - The wired Network.
- **Integration** - Provides a MAC framing service to the AP.
  - Translates the 802.11 format to the wired LAN format.
  - Translates the wired LAN format to the 802.11 format.

Wireless and Wired Networks: example



Wireless Implementation

- Security
  - Employ **VPN** with IPSec.
  - apply **RF containment**
- Security policy should at least define:
  - Wireless stations are **untrusted** external hosts.
  - A closed system based on physical security (closed system only responds to legitimate or registered entities).
  - **Vulnerability** detection and assessment procedures and techniques.
  - Policy for peer-to-peer communications and Internet Relay Chat or some new protocol that your system may not be able to securely deal with it.
- Implement IDSs and Firewalls.
  - Network Based Intrusion Detection System and Firewalls are important.
- Implement
  - Network Management,
  - Network Monitoring,
  - Network Logging,
  - SSH and SSL.

Wireless Implementation

- Roaming between access Points.
  - Uses a single IP subnet backbone for the Wireless Stations.
  - Employs **IP Mobility**.
- IP address assignment via DHCP.
  - Uses a single **DHCP server** on the backbone to service the WSs.
  - Needs to establish a backup DHCP.
  - **Static Address** assignment is an option
- Authentication: Can employ the following for authentication.
  - Remote Authentication Dial-in User Service (**RADIUS**).
  - **MAC filtering**
  - **Secure Tokens**
  - **Private and group key management systems**

Wireless Implementation (e.g)

- **Service Set Identifier (SSID)**
  - The SSID is associated with one or more APs.
  - It acts as a crude password.
- **MAC Address.**
  - The AP maintains a list of authorized MAC addresses.
  - Normally used on small networks.
- **Wired Equivalent Privacy (WEP)**.
  - RC-4 encryption with either 64 bits or higher.
  - Stops casual eavesdropping but not a concerted attack.
  - Most organisations supplement this with VPNs, Firewalls or third party software.

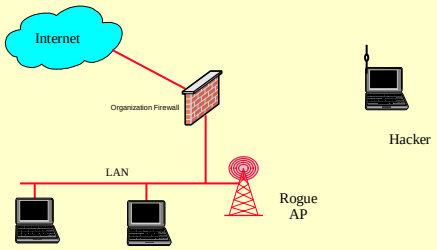
Wireless Implementation (e.g)

- WEP will only protect against casual traffic capture attacks.
- Manual Keying is a problem (even automatic key generation is still vulnerable, if keys are reused).
- WEP keys are shared - shared keys do not offer good secrecy.
- If confidentiality is important then use:
  - IPSec,
  - SSL or
  - 802.11i
- Use RADIUS to manage the keys and to provide better authentication.
- Put the wireless network outside your firewall? Or use wireless firewalls?

Wireless Problems

- New Threats.
  - Anonymous uncontrolled radio coverage areas.
  - Roaming end point mobility
  - Attacks on crypto algorithms with powerful computers
- Known Risks.
  - Unauthorised monitoring.
  - Jamming.
  - Client-to-Client attacks.
  - Brute force attacks on AP password.
  - Encryption attacks.
  - Passively intercept and decode transmitted data.
  - Attacker can be up to 20 miles from target
  - Misconfigurations

Wireless Problems : Examples



Wireless Problems : Examples

- Access Points normally ship in an unsecured configuration to emphasise ease of use and installation.
  - **Server Set Identification (SSID)**
    - Cisco "**abc**"
    - 3Com "**123**"
    - Linksys "**liksys**"
  - **Wired Equivalent Privacy (WEP)**
    - APs normally ship with WEP turned off
    - 40 and 128 bit encryption are subject to known flaws.
  - **SNMP Community passwords**
    - Many are set to "**public**"
    - 3Com"**comcomcom**"

Wireless Security Countermeasures

- Physical security considerations.
- Update the risk analysis.
- Update the network security policy.
- Access point placement and authentication.
- Implement Wireless Equivalent Privacy with enhanced security.
- Implement MAC filtering.
- Implement protocol filters.
- Implement a closed system.
- Assign static IP Addresses where possible
- Employ firewalls.
- Employ IDSs.
- Employ VPNs.
- Educate the users.
- Wireless network audit (extremely important)

Physical Security Considerations

- Conceal APs from sight.
- Keep APs away from employees.
- Properly secure outside APs.
- Properly name access points for troubleshooting.
- Enhance AP authentication.
- Ensure RF containment.
  - Sector network areas with directional antennas.
  - Metallic paint on walls.
  - Metallic foil inside walls.
  - Metallic window blinds.

Wireless Security Policy

Create wireless security policy and implement it:

- Wireless Accessibility.
  - Use Default settings?
  - Use Remote Access Dial-In User Service (RADIUS)?
  - Employ SSID, MAC Filtering, WEP encryption?
  - Employ filtering protocols?
  - Use IPSEC?
  - Implement closed systems?
- employ IDSs?
- employ firewalls?
- Lost/stolen wireless stations?
- Employ stronger encryption algorithms?
- Allow/not allow data storage on wireless stations?

Access Point Choice/Placement

- Choosing
  - an AP (capabilities vs threat analysis).
  - Closed System,
  - 128 bit WEP,
  - compatibility,
  - VPN?
- Migration to other WLAN standards for better AP protection.
- Secure placement and enhance AP authentication.
- Avoid antennas if possible. If not, perform an exhaustive RF analysis.

Current WEP Implementation

- WEP against eavesdropping **not confidentiality (f**or situation requiring confidentiality look for other solutions such as VPNs).
- WEP comes with: No encryption, 40 and 128 bits.
  - 128 bit is the minimum for a corporation but still vulnerable.
- It employs RC4 encryption algorithm but there are still rooms for security improvement.
- A 24 bit Initialisation Vector (IV) is used for each transmitted frame – vulnerable and hashing should be employed.

Implement MAC Filtering

- A unique 48 bit hexadecimal number identifying a hardware address.
- Inventory each WLAN MAC and configure the switch/AP to accept it while rejecting all others.
  - Implement MAC filtering on either the router or the AP.
- Implement MAC filtering in conjunction with
  - Logging.
  - Time of MAC access.

Implement Protocol Filtering

- Implement protocol filters on the routers or access devices at the edge of the network.
- Rules can be based upon:
  - Port number
  - Protocol type
- Restrict Ports and Protocols based upon policy.
  - Filter ICMP to prevent DoS.
  - Filter FTP and Telnet to prevent configuration alteration.
  - Filter on music to conserve bandwidth.
- Test the filters before implementing them.

Implement a Closed System

- A ***closed system*** AP does not respond to an ***"any"*** or ***null*** SSID transmitted from the client.
- ***A closed system*** AP does not broadcast to clients.
  - The AP **challenges** the client for its SSID.
  - If the client broadcasts an ***any or null*** the AP does not respond.
- The SSID should be a name that is hard to guess.
- A closed system negates snooping by ***Netstumbler***.

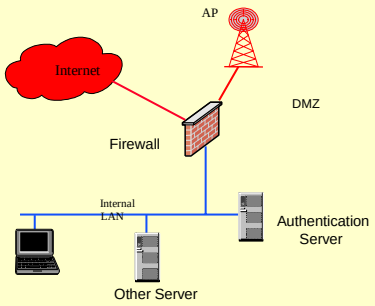
IP Address Deployment

- Wireless transmission encompasses the Physical and Data link layers.
- IP sits on top of these two stacks and provides a seamless interface to the wired LAN.
  - IP security tactics can be as effective in the WLAN as in the LAN space.
- IP address can be assigned either statically or with DHCP.
  - DHCP IP assignment is easier to manage but does announce the network.
  - Static IP assignment is harder to manage but hides the network.

Wireless LAN and Firewalls

- Install a firewall to separate the DMZ from the internal network.
- Install a firewall to separate the DMZ from the external network.
- Install a personal firewall on all individual hosts.
- Filter both inbound and outbound connections.
- Activate and check logging regularly.

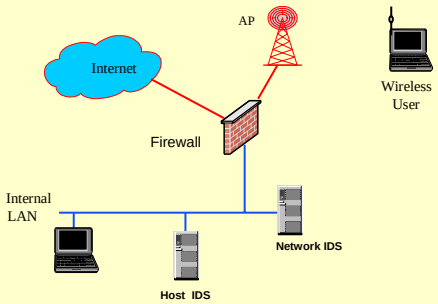
Firewall and DMZ



Wireless LAN and IDS

- Install a NIDS on the wireless DMZ
- Install a HIDS on selected servers.
  - Log file monitors
  - Integrity monitors
  - Signature scanners
  - Anomaly detectors
  - Activate and check logging.

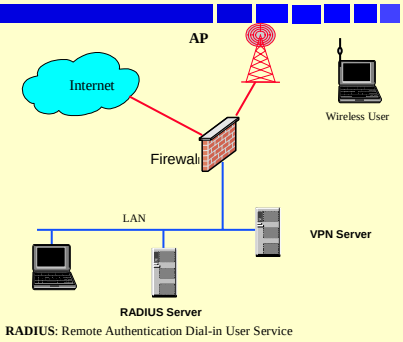
Wireless LAN and IDS



Wireless LAN and VPN

- Provides for Point-to-Point encryption and authentication.
- The VPN server on the LAN can provide both the authentication and the encryption requirements.
  - In practice the RADIUS performs the authentication while the VPN provides the encryption.
- Multiple key changes over time.
- Mobile IP should be employed with VPN to provide confidentiality and prevent dropping during roaming.

Virtual Private Network



RADIUS: Remote Authentication Dial-in User Service

Wireless Security Guidelines

- An **AP** is a **REMOTE** Access Service!
  - Do not use the defaults.
  - Filter on MAC addresses.
  - Define standard AP configurations.
  - Search for unauthorised APs using AP auditing tools.
  - Conduct regular AP security audits and penetration tests.
- Protect the **Wireless Client**.
  - Provide specified IP ranges for WLAN.
  - Force wireless users to install personal firewalls
  - Enforce security of services for wireless clients with VPN.

Wireless Network Vulnerabilities

- Packet sniffing.
- Insertion attacks.
- WEP isn't secured (well-known problem).
- Rogue access points (very common and serious problem).
- Misconfiguration (you will say everyone makes mistakes so do I!).
- Standard attacks (known techniques to attack wired networks).
- Crypto attacks (very serious, now and in the future).

Wireless Network Tools

- **Airsnort**
  - **recovers encryption keys; it operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.**
- **Netstumbler**
  - **site surveys, detecting rogue access points, and finding and mapping WLAN installations.**
- **Kismit**
  - **capable of sniffing using most wireless cards, automatic network IP block detection via UDP, ARP, and DHCP packets.**
- **NetStumbler:**
  - **Wireless network scanning tool.**

Some Tips

- **AP Changes**
  - **Use directional antennas**
  - **Lower the transmit power**
  - **Apply password policy**
  - **Change WEP keys often**
  - **Apply MAC address filtering**
  - **Disable SSID or make changes periodically**
  - **Disable broadcast pings**
  - **Disable DHCP**
  - **Change subnet address range**
- **Replace hubs with switches**
  - **Can help prevent snooping**

Some Tips

- **Use 3rd party products to enforce security (NOT always a good idea)**
  - **EcuTel**
    - **Provides a secure communication protocol well above WEP standards**
- **Employ new standards with stronger authentication.**
  - **802.11x**
    - **Port control**
    - **Extensible Authentication Protocol (EAP), PEAP, etc.**
    - **Stronger WEP**
    - **Temporal Key Integrity Protocol (TKIP)**
  - **Apply ECC in applications and on authentication servers**