Wireless Networks: Basics and Auditing

Ed Crowley

Fall 09

Qualifications

- NSA Information Security (INFOSEC) Certifications :
  - Assessment Methodology (IAM)
  - Evaluation Methodology (IEM)
- Designed NSA/NTISSI Certified (4011, 4014) Security Specialization at UH, College of Technology.
- Dozen+ earned certificates from the usual suspects ISC^2, Cisco, Microsoft, Novell, CompTIA…
- Former IS Director, Network Administrator, Heathkit/Zenith Educational Media Designer …
- US Army, Military Police Academy Graduate ('70)
  - German Shepherd Sentry Dog Handler

Everything that I needed to know about Cyber Security, I learned from my

German Shepherd Sentry Dog …

Sentry Dog Rules

- Be polite.
- Be professional.
- Have a plan to kill everyone you meet.

Today’s Topics

- Wireless Networking
  - Drivers and Vulnerabilities
- IEEE 802.11 Family
- WLAN Operational Modes
- Wired Equivalent Privacy (WEP)
- WPA and WPA2
- Authentication Protocols
- WLAN Threats
- Wireless Hacking (Auditing) Tools
- Securing WLANs
- Bluetooth Overview

Wireless Growth Drivers

1. Convenience
2. Cost

Related Laws

- Gilder's Law
  - Total bandwidth of communication systems triples every twelve months.
- Metcalfe's Law
  - Value of a network is proportional to the square of the number of nodes.
    - As a network grows, the value of being connected to it grows exponentially, while the cost per user remains the same or even reduces.

Wireless Growth Vulnerabilities

- At home, your next door neighbor, with a UHF scanner, may listen to your cordless phone calls.[1]
- At the coffee shop, the person next to you might sniff your wireless connection.
  - Stealing your credit card numbers, passwords...

Conclusion

- Open broadcast infrastructures of Wireless LANs (WLANs) are relatively vulnerable.

1. For the last decade or so, it has been illegal for a nongovernmental person to purchase a scanner with these capabilities…

Governmental Regulations

- In US, wireless regulated by FCC.

http://wireless.fcc.gov/index.htm?job=rules_and_regulations

- Governmental supervision means that:
  - Wireless systems that in different countries may operate on different frequencies
  - Allocated wireless frequencies often don’t match the frequencies allocated in other countries.

Industrial, Scientific, and Medical Bands

- WLANs can operate in three areas of the radio spectrum, referred to as the Industrial, Scientific, and Medical (ISM) bands.
  - Originally, industrial, scientific and medical (ISM) radio bands were reserved internationally for the use of RF electromagnetic fields for industrial, scientific and medical purposes rather than for communications.
  - In general, communications equipment must accept any interference generated by ISM equipment.
    - 802.11b operation falls under the ISM mandate while 802.11a operation falls under the National Information Infrastructure (U-NII) mandate

Cellular Phone Network

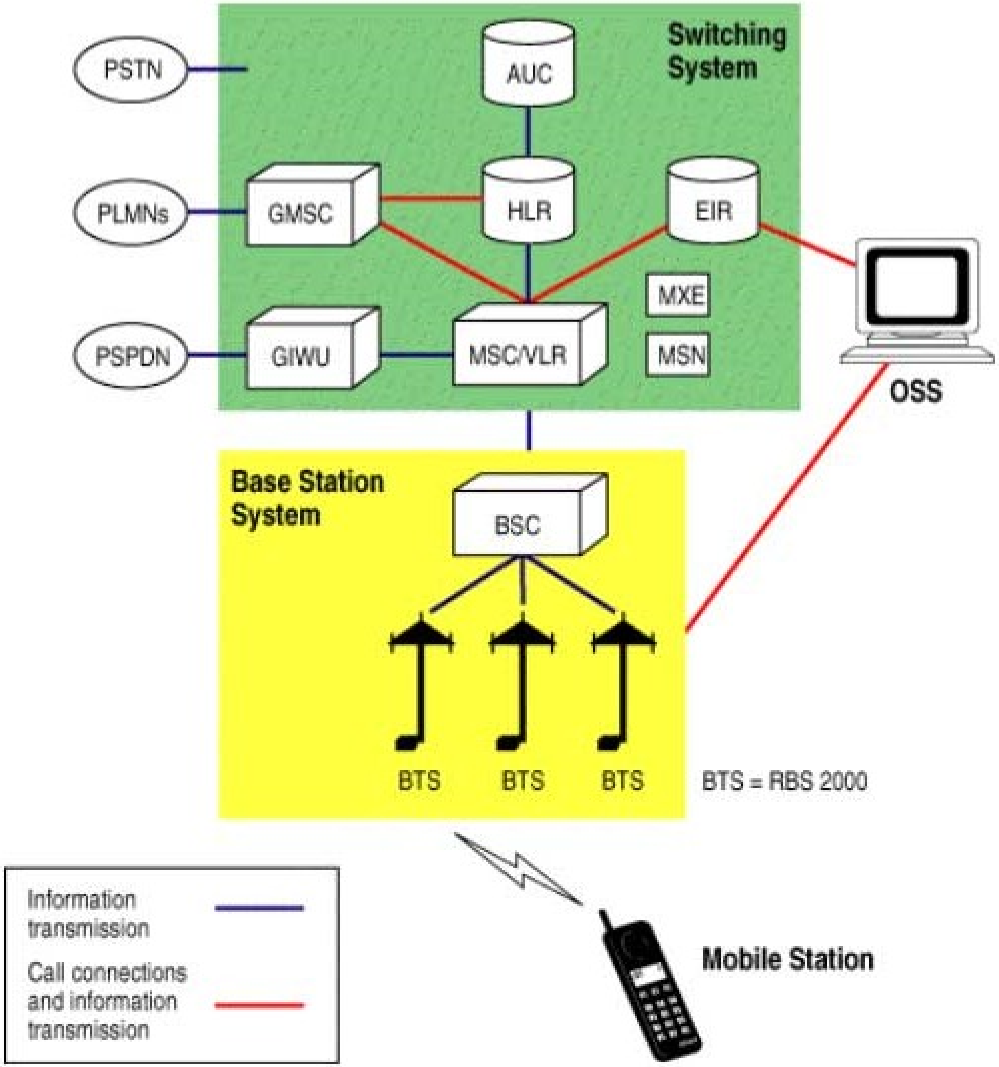
- A radio network made up of a number of radio cells (or just cells) each served by at least one fixed-location transceiver known as a cell site or base station.
- Two developments improved radio telephone service

1. Advances in UHF Radio
2. Advances in computing

Worldwide Cellular via LEO Satellites

- Besides extending basic voice coverage to new customers, Low Earth Orbit (LEO) can offer advanced services, such as Internet access and video.
  - LEO systems use the same interface technologies as today’s digital wireless networks.
  - Some use code division multiple access (CDMA) while others employ a variation on time division multiple access (TDMA) technology.
- Medium Earth Orbit (MEO) satellites can also be used for communications
  - ❑ Begins at about 12,000 km

Cellular Network Elements



- Cell Tower
- Base Station Controller (BSC)
- Mobile Switching Center (MSC)
- Visiton Location Register (VLR)
- Home location Register (HLR)
- Mobile Identity Number (MIN)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- Operations and (OMC) Maintenance Center

Global Wireless Transmission Systems

Globally several different transmission systems are used for cellular telephone service including:

- AMPS Advanced Mobile Phone Systems
  - – US standard for analog cellular service (1G)
- TDMA Time Division Multiple Access
  - – First US digital standard. (2G)
- CDMA Code Division Multiple Access
- GSM Global System for Mobile Communications (GSM) Most widely deployed digital network in the world.
- CDPD Cellular Digital Packet Data

Global Wireless Transmission System Examples

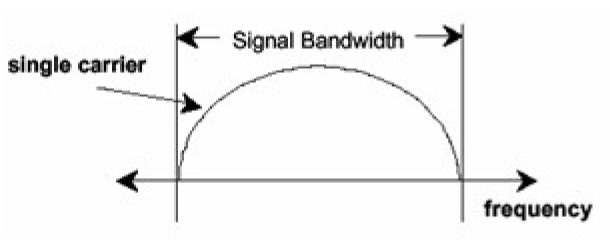
- NMT Nordic Mobile Telephone – Original Japanese standard for analog cellular service
- TACS Total Access Communication System -- An analog FM communication system used in some parts of Europe and Asia (1G)
- PDC Personal Digital Cellular – A TDMA based Japanese standard OS, operating in the 800 and 1500 Mhz bands. (2G)
- General Packet Radio Services (GPRS) – An IP based packet-switched wireless protocol that allows for burst transmission speeds of up to 1.15Mbps
- Enhanced Data Rates for Global Evolution (EDGE) -- A higher bandwidth version of GPRS.

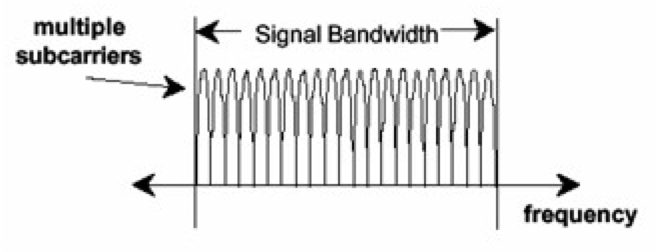
Wireless Networking

- Spread Spectrum the de facto wireless LAN communication standard.
  - Broadcasts signals over a range of frequencies.
  - Originally developed for military use to provide secure, mission-critical communications.
- Provides some immunity to interference associated with narrowband systems.

RF Technologies

- Different spread spectrum RF technologies for Wireless LANs:
  1. Direct Sequence Spread Spectrum (DSSS)
  2. Frequency Hopping Spread Spectrum (FHSS)
  3. Orthogonal Frequency Division Multiplexing (OFDM) a multi-carrier modulation scheme where data is split up among several closely spaced subcarriers.
  4. MIMO--multiple-input multiple-output





IEEE 802.11 Family

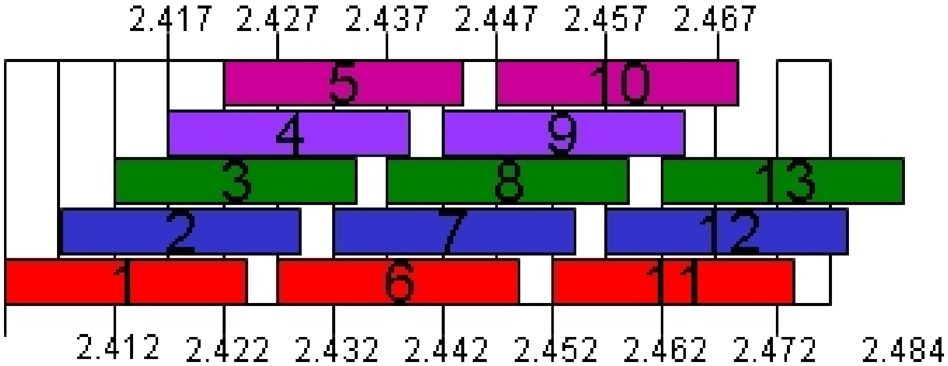
- Most popular wireless LAN standards.
  - 1997, IEEE accepts 802.11 Specification.
  - Specifies an over-the-air interface between:
    - A mobile device wireless client and a base station or
    - Between two mobile device wireless clients.
- Wireless connection uses a subset of the radio spectrum, (aka the ISM Band).
  - ISM Bands are:
    - 902-908 MHz
    - 2.4-2.4835 GHz
    - 5.725-5.825

802.11 Standard Family

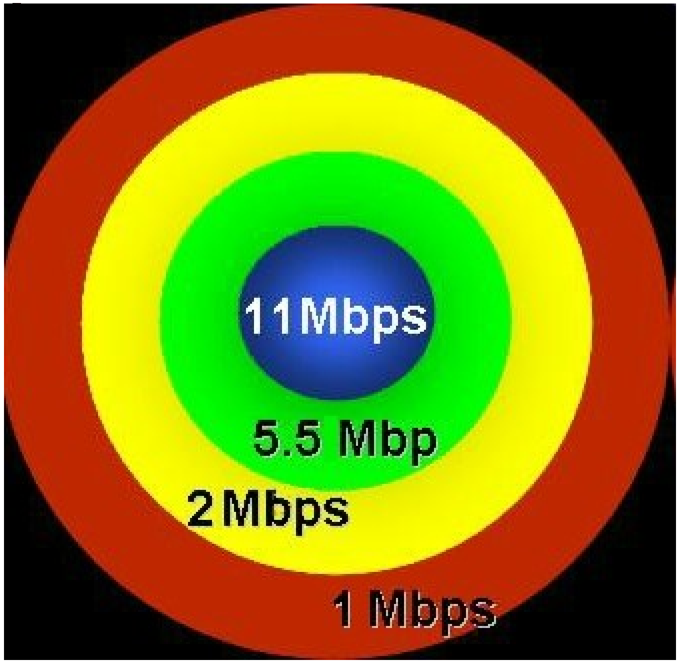
Protocol	Release	Frequency	Typical Throughput	Theoretical Throughput	Modulation	Avg. Indoor Range	Avg.Outdoor Range
802.11	1997	2.4GHz	0.9Mbps	2Mbps		20m	100m
802.11a	1999	5GHz	23Mbps	54Mbps	OFDM	35m	120m
802.11b	1999	2.4GHz	4.3Mbps	11Mbps	DFSS	38m	140m
802.11g	2003	2.4GHz	19Mbps	54Mbps	OFDM	38m	140m
802.11n*	Est 2009	2.4/5GHz	X	248Mbps	MIMO	70m	250m

*DRAFT STANDARD

802.11 Spread Spectrum Channels and Throughputs



Channels



Available Throughputs

802.11 Standard

- Specifies physical and medium access control (MAC) network layer attributes.
- Physical layer responsible for transmission of data among nodes.
  - Can use direct sequence spread spectrum, frequency hopping spread spectrum or infrared pulse position remodulation.
- MAC Layer consists of a set of protocols responsible for maintaining order on the shared medium.
- IETF specifies upper two levels.

MAC Layer Services

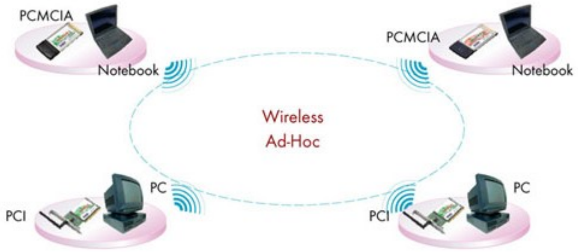
- Data transfer
  - CSMA/CA Carrier Sense Multiple Access/Collision Avoidance
- Association
  - In Infrastructure mode, establishes wireless links between wireless clients and access points
- Re-association
  - Takes place when a wireless client moves from one Basic Service Set (BSS) to another
- Authentication
  - Proves a client’s identity through the use of the 802.11 Wired Equivalent Privacy (WEP)
  - Shared key configured into the access point and its wireless clients.

802.11 MAC Layer Services (cont)

Privacy

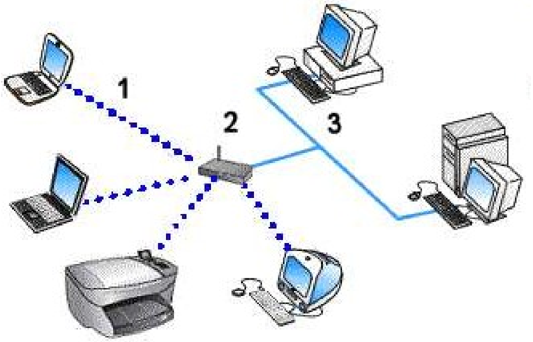
- By default, data transfers in the clear.
- WEP implements an encryption process.
  - RC-4 in output feedback mode
    - For encryption, secret key shared between mobile station and base station access point …
    - Flawed implementation …
  - For integrity, uses a CRC-32 checksum
  - No protection against replay attacks

802.11 WLAN Operational



Ad Hoc Mode

- Denotes a mesh wireless network where the computers are connected in a peer to peer topology.



Infrastructure Mode

- Centered around a wireless access point (WAP). A WAP is a centralized wireless device that controls the traffic in the wireless medium.

Association Frames

- Before communicating data, mobile wireless clients and access points must establish a relationship, or an association.

Three Possible States

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authenticated and associated

Service Set Identifier (SSID) and Basic Service Set

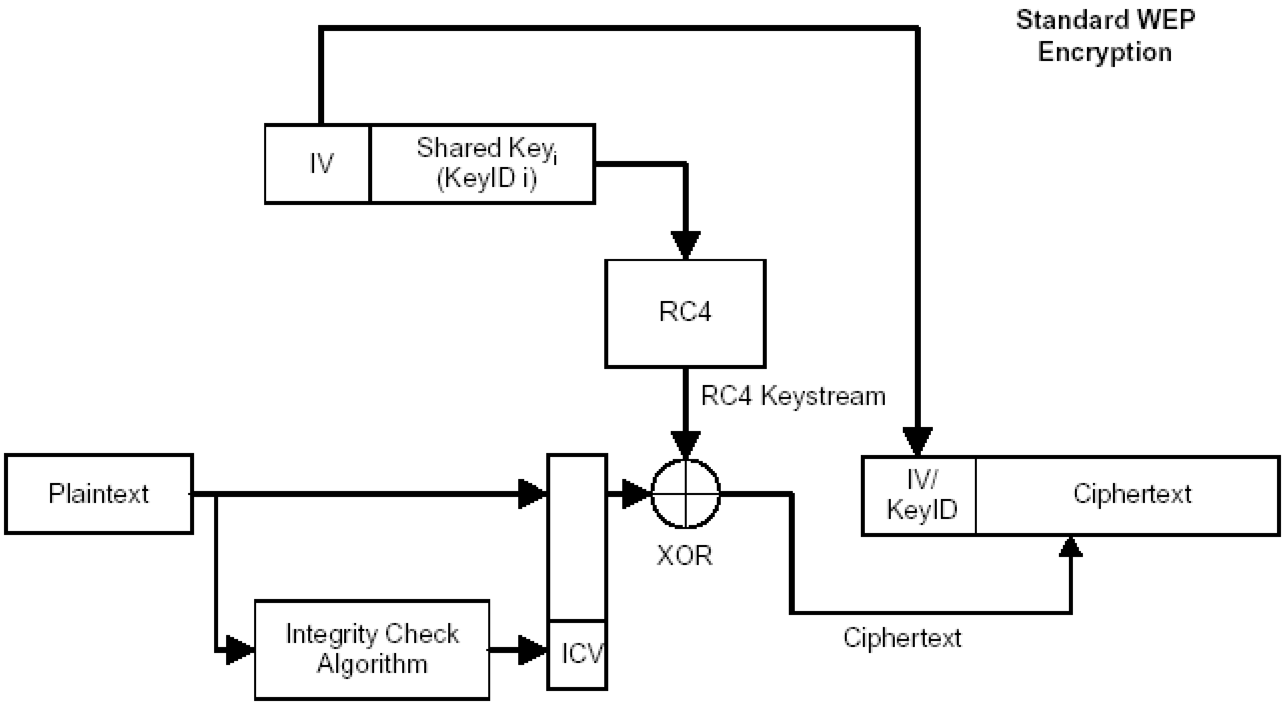
- In addition to traditional network settings, the channel and service set identifier must be configured for a WLAN to function.
- SSID is an alphanumeric string that differentiates networks operating on the same channel and functions as a unique identifier.
- In infrastructure mode one access point (AP) together with all associated stations (STAs) is called a Basic Service Set (BSS).
  - Each BSS is identified by an BSSID.
  - In infrastructure mode, a basic BSS consists of at least one AP and one STA.....

Wired Equivalent Privacy (WEP)

- Mechanism for securing wireless LAN data streams.
  - Part of original 802.11 standard.
  - Utilized RC 4.
- Symmetric scheme where the same key and algorithm both encrypt and decrypt.
  - To encrypt, keystream is X0Red with plaintext.

RC-4/WEP Encryption Process

Figure 1. Standard WEP Encryption Process



WEP Goals

Access control

- Prevents users lacking WEP key from gaining network access

Privacy (Confidentiality)

- Protects wireless LAN data streams by encrypting them and allowing decryption only by users with correct WEP keys

WEP Authentication Methods

- A client cannot participate in a wireless LAN until after client is authenticated.

Two types

1. Open
    - Open, the default authentication protocol, authenticates any request.
1. Shared Key
    - Considered a null authentication

Shared Key Authentication

- Utilizes a shared secret key to authenticate station to AP.
  - – Uses:
    - Standard challenge and response
- Anyone without assigned key is denied access.
  - Same shared key encrypts and decrypts data frames
    - Note, this is considered a security risk

WEP Key Management

- Shared key resides in each station's management information database (mib).

Two schemes

1. A set of four default keys are shared by all stations, including the wireless clients and their access points.
2. Each client establishes a key mapping relationship with another station

WEP Cracking

Popular attacks include:

- Passive attacks to decrypt traffic based on statistical analysis
- Active attacks to inject new traffic from unauthorized mobile stations based on known plaintext (ARPs)
- Active attacks to decrypt traffic based on tricking the access point
- Dictionary-building attacks that, after an analysis of about a day’s worth of traffic, allow real-time automated decryption of all traffic.

WPA and WPA2

- WPA instant response to WEP flaws
- WPA2 part of 802.11i standard
- Attempts to address WEP’s security flaws
  - Consists of two encryption approaches: TKIP/MIC and AES-CCMP

802.11 Supports RADIUS

- Remote Authentication Dial In User Services (RADIUS) and Kerberos
- Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected.
- After successful authentication, normal traffic can pass through the port.
- Also supports EAP, EAP-TLS, and LEAP.

WLAN Threats

- Denial of Service Attacks
  - Many potential vectors.
    - For example, Microwave ovens operate in the 2.4 GHz range
- SSID Problems
  - Default
- The Broadcast Bubble
  - Extends past your building
- War Driving
- Rogue Access Points
- MAC Spoofing

Wireless Hacking Tools

Kismet

- Layer 2 wireless network detector, sniffer, and intrusion detection system.
- Sniffs 802.11 a, b, and g traffic

NetStumbler

- Functions as a high level WLAN scanner.

WEPCrack

- Open source tool for breaking 802.11 WEP secret Keys.

Wireless Hacking Tools

AirCrack

- WLAN and WEP auditing tool.

Securing WLANs

- Includes strategies for MAC address filtering, firewalls or a combination of protocol based or standards based measures.

Standards and Policy Based Solutions

- Address ownership and control of wireless

MAC Address Filtering

- Time consuming, limited effectiveness.

Securing WLANs

SSID Solutions

- If the SSID is set to manufacturers default settings, it often means that the other measures are also at default.
- SSID should not reflect company's name, division, or products.

Antenna Placement

- Should be incorporated into site survey and site updates

Other Measures

- VLANS
- VPNs
- Wireless RADIUS
- Dynamic WEP Keys

Want Security? Don’t use WEP

- Enable WPA2
- Employ regular scans to find rogue access points.
- Consider network based Intrusion detection on the wireless LAN
- Employ Logging

Bluetooth

- A simple peer to peer protocol created to connect multiple consumer mobile information devices (cell phones, laptops, printers, cameras,…)
- Whenever any Bluetooth enabled devices come within range of each other, they instantly transfer address information and establish small networks between each other, without the user being involved.

Questions?