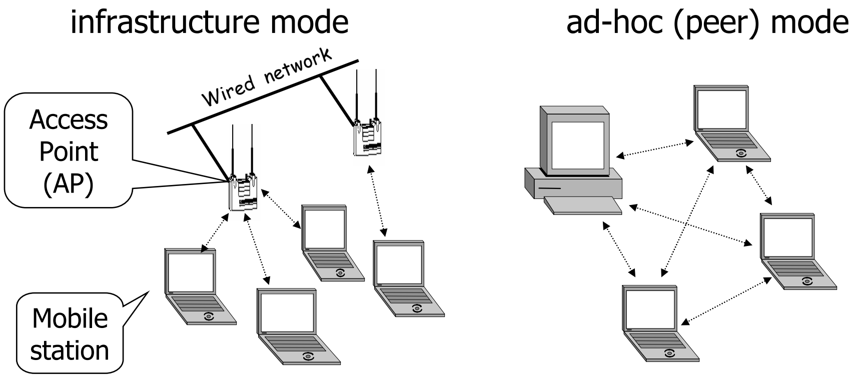
# The 802.11 Standard

- Specifies LAN networking functions over “air” (ether)
- 802.11 is composed of
  - Medium Access Control
  - Physical Layer


infrastructure mode

ad-hoc (peer) mode

# Common Wireless Technologies

- Regulated by IEEE 802.11x Standards Body
  - 802.11a
  - 802.11b
  - 802.11g

  Coming soon…
  - 802.11n

# 802.11a

- Works at 40mhz, in the 5ghz range
- THEORETICAL transfer rates of up to 54mpbs
- ACTUAL transfer rates of about 26.4mbps
- Limited in use because it is almost a line of sight transmittal which necessitates multiple WAP's (wireless access points)
- Cannot operate in same range as 802.11b/g
- Absorbed more easily than other wireless implementations

# 802.11b – "WiFi"

- Operates at 20mhz, in the 2.4ghz range
- Most widely used and accepted form of wireless networking
- THEORETICAL speeds of up to 11mbps
- ACTUAL speeds depend on implementation
  - 5.9mbps when TCP (Transmission Control Protocol) is used (error checking)
  - 7.1mbps when UDP (User Datagram Protocol) is used (no error checking)
- Can transmit up to 8km in the city;
  rural environments may be longer if a line of sight can be established

# 802.11b - “WiFi” (cont.)

- Not as easily absorbed as 802.11a signal
- Can cause or receive interference from:
  - Microwave ovens (microwaves in general)
  - Wireless telephones
  - Other wireless appliances operating in the same frequency

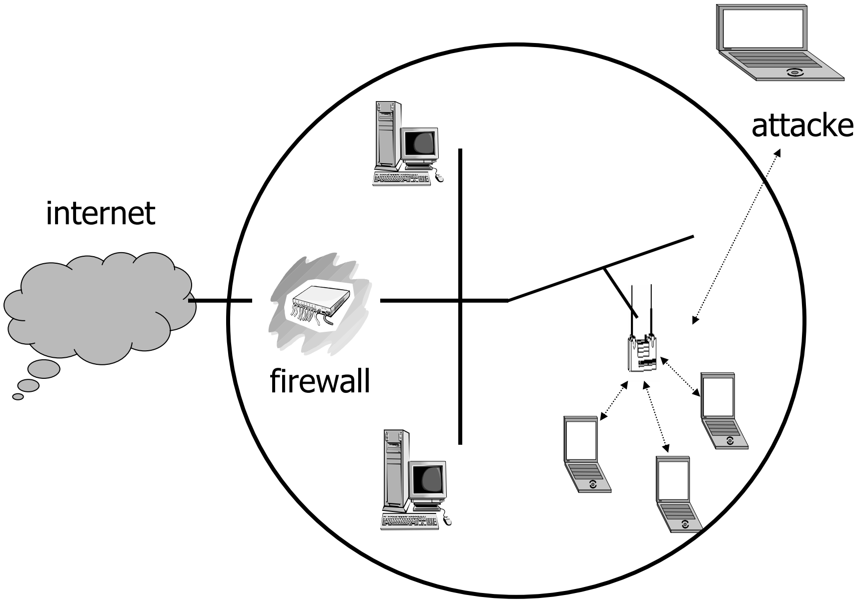
# 802.11g - “Super G”

- Operates at the same frequency range as 802.11b
- THEORETICAL throughput of 54mpbs
- ACTUAL transmission rate is dependent on several factors, but averages 24.7mbps
- Logical  upgrade from 802.11b wireless networks – backwards compatibility
- Suffers from same limitations as 802.11b network
- System may suffer significant decrease in network speeds if network is not completely upgraded from 802.11b

# 802.11n (Ultranet)

- Standards in discussion now;  should be completed by the end of 2006
- REAL throughput of at least 100mbps
  - 4 – 5 times faster than 802.11g/a
  - 20 times faster than 802.11b!
- Better distance than 802.11a/b/g
- Being designed with speed and security in mind

# The Parking Lot Attack



# 802.11 Security

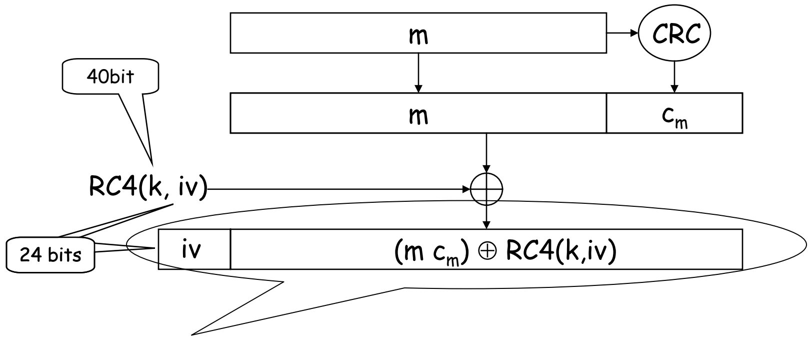
- Goals
  - primary goals : confidentiality
  - other goals :
    - access control
    - integrity
- Mechanisms
  - open system “security”
    - allow anyone
    - plaintext transmission
  - shared key based security (using WEP)
    - authentication, encryption/decryption

# WEP

- Wired Equivalent Privacy
  - protecting authorized users of a wireless LAN from casual eavesdropping
- Properties
  - reasonably strong ???
  - self-synchronizing
    - link level encryption/decryption protocol
  - efficient
  - exportable

# WEP Protocol (encryption)

- m : message    $c_m$ : integrity checksum
- k  : shared key
- iv : initialization vector (randomly chosen)

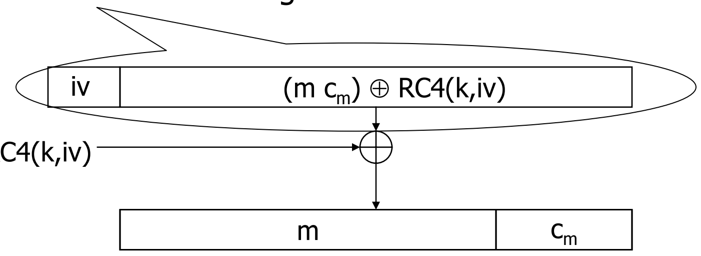


ciphertext : transmitted through the radio link

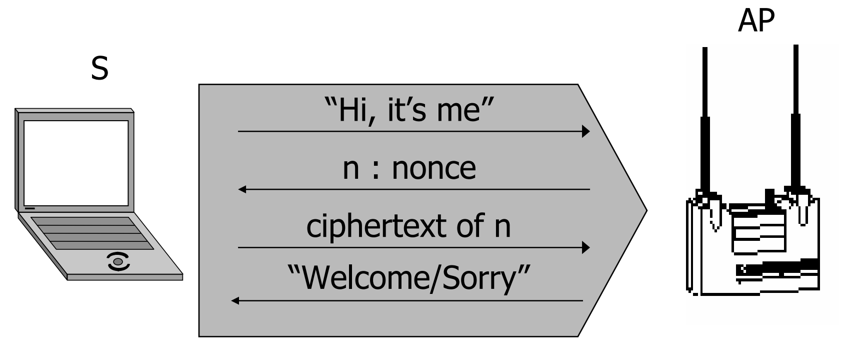
# WEP Protocol (decryption)

- m : message    $c_m$ : integrity checksum
- k  : shared key (distribution is not mentioned)
- iv : initialization vector (randomly chosen)

ciphertext : received through the radio link



# Authentication using WEP



S

AP

"Hi, it's me"

n : nonce

ciphertext of n

"Welcome/Sorry"

# Attacking WEP Keys

- Papers
  - Weaknesses in the Key Scheduling Algorithm of RC4
    - S. Fluhrer, I. Mantin, and A. Shamir, SAC 2001
  - Using the Fluhrer-Mantin-Shamir Attack to Break WEP
    - A. Stubblefield, J. Ioannidis, A. Rubin
- Philosophy
  - RC4 has many weak KEYS (WEP key plus IV)
  - Knowledge of a small number of key bits suffices to determine many states and output bits with non-negligible probability.

# Attacking WEP Keys (Cont.)

- mounting the attack:
  - search for IV that leaks information about the WEP key
  - a packet just leaks a little info on the WEP key
    - millions packets to recover a 128-bit key

# Attacking the “holes” of WEP

- Intercepting Mobile Communications: The Insecurity of 802.11
  - N. Borisov, I. Goldberg, D. Wagner

- Attack based on Keystream Reuse
  - two ciphertexts obtained by using same values of (iv, k) reveal information about their plaintexts

Let: $C1 = P1 \oplus RC4(iv,k)$

$C2 = P2 \oplus RC4(iv,k)$

=> $C1 \oplus C2 = P1 \oplus P2$

  - we can obtain P1 if we know P2

# Attack based on Keystream Reuse

- assuming fixed k, known plaintext, we could build Decryption Dictionaries

| | | | | |
|---|---|---|---|---|
| C | = | RC4 (iv, k) | XOR | <M, c(M)> |
| P | = | < M, c(M) > | | |
| C XOR P | = | RC4 (iv, k) | | |

  - number of entries is $2^{24}$, each entry occupying about 1500 bytes, which roughly totals 24 GB
  - building this table ensures decryption, even if length of k is increased
  - most access point reset iv to 0 when powered on and increase by 1

# Attacks on Checksum

- property 1 (of WEP CRC-32 checksum)
  - $c(x \oplus y) = c(x) \oplus c(y)$

- message modification

$C = RC4(iv, k) \oplus <M, c(M)>$

to modify $P(<M, c(M)>)$ into $P \oplus \Delta$,

$C' = C \oplus <\Delta, c(\Delta)>$

$= RC4(iv, k) \oplus <M, c(M)> \oplus <\Delta, c(\Delta)>$

$= RC4(iv, k) \oplus <M \oplus \Delta, c(M \oplus \Delta)>$

# Attacks using Checksum

- property 2 (of WEP CRC-32 checksum)
  - it is an un-keyed function of the message
- property 3 (of WEP access point)
  - it is possible to reuse old IV values without triggering any alarms at the receiver

- message injection
  - given random M, generating c(M) using property 2
  - C = RC4(iv, k) $\oplus$ <M, c(M)>
  - send out using property 3
  - a special case: authentication spoofing

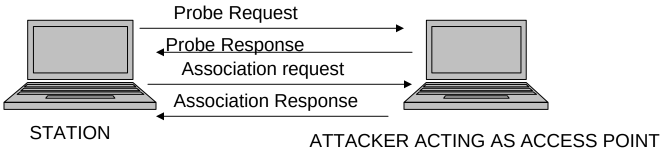
# Closed Network Access Control

- SSID : service set identifier
  - only someone who knows SSID can be served
  - but, SSID is typically broadcasted in the clear

- Ethernet MAC Address Access Control Lists
  - only wireless card with listed MAC address can be served
  - unfortunately, MAC addresses are also sent in the clear over the air → trap and clone!!!
  - wireless card MAC address clone

# Rogue Access Point

- Attacker acting as access point.



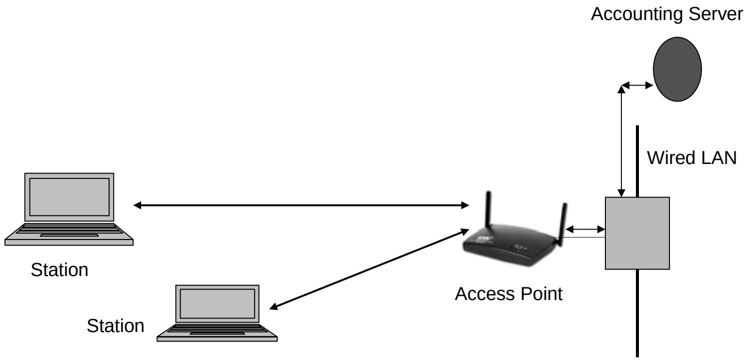
- Can be easily done using Freeware tools like HostAp
- Problem: Station gives all its information to the attacker.
- Solution: Airwaves should be monitored continuously to see client connect to authorized access points.

# Jamming (DoS)

- Since WLAN works on 2.4GHz frequency, it shares this medium with various other devices like microwaves, cordless phones, etc.

- Problem:
  - Attacker can easily flood the access medium.
  - Attacker can act as an access point and continuously flood airwaves with disassociate frame using access point's MAC address, thus forcing stations to disconnect from the LAN.

# Typical implementation



# More Information

- Hacking tools
  - to crack the key
    - http://airsnort.sourceforge.net/
    - http://sourceforge.net/projects/wepcrack/
  - wireless sniffers
    - http://www.personaltelco.net/index.cgi/WirelessSniffers
- New security standard
  - 802.11i: http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
  - http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf