WIRELESS SECURITY

Information Security in Systems & Networks

Public Development Program

Sanjay Goel

University at Albany, SUNY

Fall 2006

Wireless LAN Security

Learning Objectives

- Students should be able to:
  - Understand how WiFi works.
  - Identify various wireless attacks including eavesdropping, denial-of-service, man-in-the-middle, and ARP poisoning.
  - Determine relevant security controls required for specific WiFi attacks.

Wireless

Wi-Fi Process

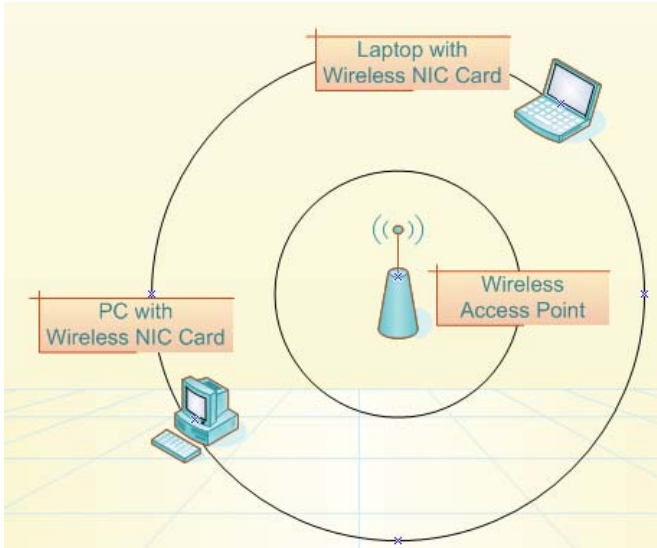
- Access points transmit a beacon at a fixed interval
- To connect through the access point the mobile device listens for beacon to identify access points in range
  - The mobile device selects the network to join
  - The device may also send a probe request to identify a specific access point affiliated with a desired service set Identifier (SSID).

    (An SSID is an identification value programmed into a wireless access point.)

Wireless

Wi-Fi Process Cont'd.

- After the access point is selected, the device and the access point perform mutual authentication
- Following authentication the device sends an association request to which the access point responds
- The mobile client becomes a peer on the wireless network, and can start transmitting data on the network.



Wireless Insecurity

Wireless Attacks

- Passive Attacks
  - War Driving (Locating free access points)
- Denial of Service
  - Jamming (by using a device which will flood spectrum with noise and traffic)
  - Sleep Deprivation Attacks (People run programs on wireless devices to drain the power of the device)
  - Spoofing identity (through cloning MAC address of and setting strength of signal to greater than other user)
  - Spoofed access points (clients are usually configured to associate with the access point with the strongest signal)

Wireless Insecurity

Wireless Attacks

- Man-in-the middle attack
  - Hacker inserts itself into the communication and becomes a proxy
- ARP poisoning
  - Attacker can get packets and frames from the air by "poisoning" caches of MAC/IP combinations of two hosts connected to the "physical" network.

Wireless Insecurity

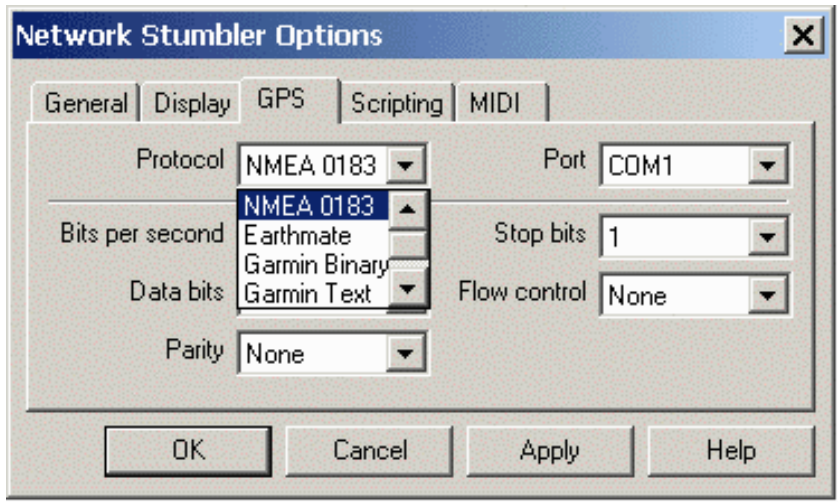
Discovering Access Points: War Driving

- Searching active wireless access points by driving through a city
  - Wireless communication takes place on unlicensed public frequencies
  - Benign act of locating and logging wireless access points is legal
- Invented by Peter Shipley and commonly practiced by hobbyists, hackers & security analysts worldwide
- Signals from wireless routers can carry up to 2000 feet allowing eavesdroppers to drive by and infiltrate the network
- Several tools available for war driving, e.g., NetStumbler, Kismet
- Wireless network adaptor that supports promiscuous mode allows hacker to capture network traffic
  - Network Monitor in Windows, TCPdump in Linux, AirSnort.

Wireless Insecurity

Netstumbler

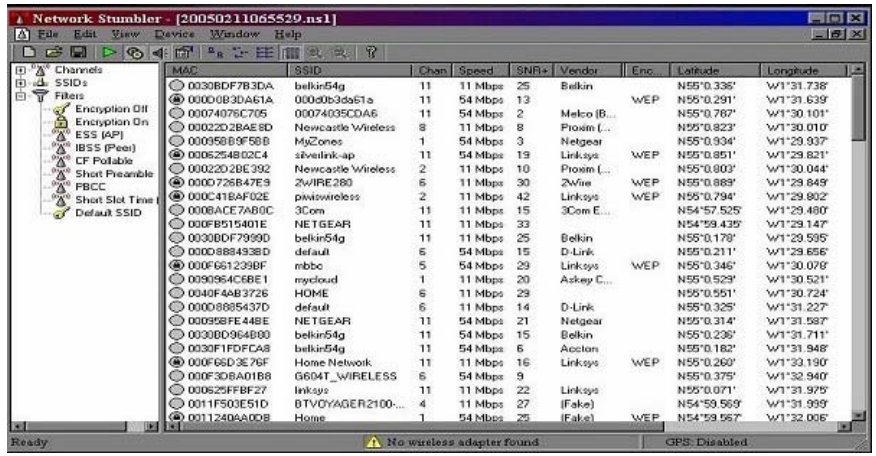
- Works primarily with wireless network adaptors that use the Hermes chipset because of its ability to detect multiple Access Points within range
  - Orinoco gold card most popular with Netstumbler
  - Hermes chipset is that it doesn't support promiscuous mode thus cannot be used to sniff network traffic.
- For sniffing traffic a wireless network adaptor that supports the PRISM2 chipset is required
  - Several cards use the Prism2 chipset, e.g. Linksys
- It can provide detailed information on the wireless networks it detects
- It can be used in with a GPS device to provide exact coordinates of the detected wireless networks.



Wireless Insecurity

Netstumbler

- Netstumbler works on networks that are configured as *open systems*.
  - i.e. the access point responds with the value of its SSID to other wireless devices when they send out a radio beacon with an "empty set" SSID.
- For protection against Netstumbler, the wireless network should be configured as a *closed system*.
  - i.e. access point does not respond to "empty set" SSID beacons and is not visible to netstumbler
  - Obtaining an SSID does not imply that the network has been compromised.
- Other packet decoding techniques such as Ethereal, AiroPeek, etc. can still be used
- RF spectrum analyzers can be used to discover the presence of wireless networks.



Wireless Insecurity

Denial of Service (Jamming)

- Jamming occurs when spurious RF frequencies interfere with the operation of the wireless network.
- Attacker analyzes the spectrum being used by wireless networks and then transmits a powerful signal to interfere with communication on the discovered frequencies.
- Requires special hardware that can transmit powerful radio frequencies
- Attack lasts only as long as the transmission is current
- Jamming may also be caused by the presence of other devices, such as cordless phones, that operate in the same frequency spectrum as the wireless network.
  - To resolve such situations policies regarding use of wireless devices in the organization are enacted.

Wireless Insecurity

Denial of Service (Spoofed MAC)

- MAC filtering allows only clients that possess valid MAC addresses access to the wireless network.
  - The list of allowable MAC addresses can be configured on the AP, or it may be configured on a RADIUS server that the AP communicates with.
- Spoofing occurs when an attacker changes his/her devices MAC address to impersonate an authorized station on a wireless network
- Relatively easy to discover authorized addresses.
  - MAC addresses are sent in the clear on wireless networks

Wireless Insecurity

Spoofing (Spoofed MAC cont'd.)

- MAC address can be changed relatively easily
  - Windows: simple edit of the registry
  - UNIX: through a root shell command.
- WEP can be deployed to provide protection against authentication spoofing through use of Shared Key authentication.
  - Both plain text challenge and cipher text is visible in this authentication allowing hackers to spoof authentication to a closed network.

Wireless Insecurity

Spoofing (Spoofing AP)

- Once the attacker knows the SSID in use by the network the hacker sets up a rouge AP with signal strength stronger than the legitimate AP
- Wireless users will have no way of knowing that they are connecting to an unauthorized AP.
- Hacker gains information, such as, authentication requests, secret key etc.
- Hacker can use two wireless adaptors (man-in-the-middle attack)
  - One card is used by the rogue AP
  - Other card is used to forward requests through a wireless bridge to the legitimate AP.
- With a strong antenna, the rogue AP can be deployed at a distance, such as, parking lot
- Protection: Periodic physical inspection of premises

Wireless Insecurity

Spoofing (Evil Twin)

- Hacker sets up his laptop as a rogue access point
  - Software is available to convert a laptop into a Soft Access Point
  - The soft access point broadcasts spoofed SSID of legitimate Access Point
  - Hacker provides a legitimate sounding name to the access point
- User connects to the rogue access point assuming it to be legitimate
- Hacker harvests personal information from the communication

Wireless Security

Sleep Deprivation Attack

- Hacker consumes resources of a device on wireless network
  - e.g. battery power, bandwidth, & CPU
- Effective because of power limitations on wireless devices
  - Prevents hibernation or stand-by
- Resource Consumption Attacks
  - **Malignant Attack:** Executable file is created or existing code is modified to increase power consumption.

    (e.g. infinite loop)
  - **Benign Power Attack:** Device executes a valid, but energy hungry task.

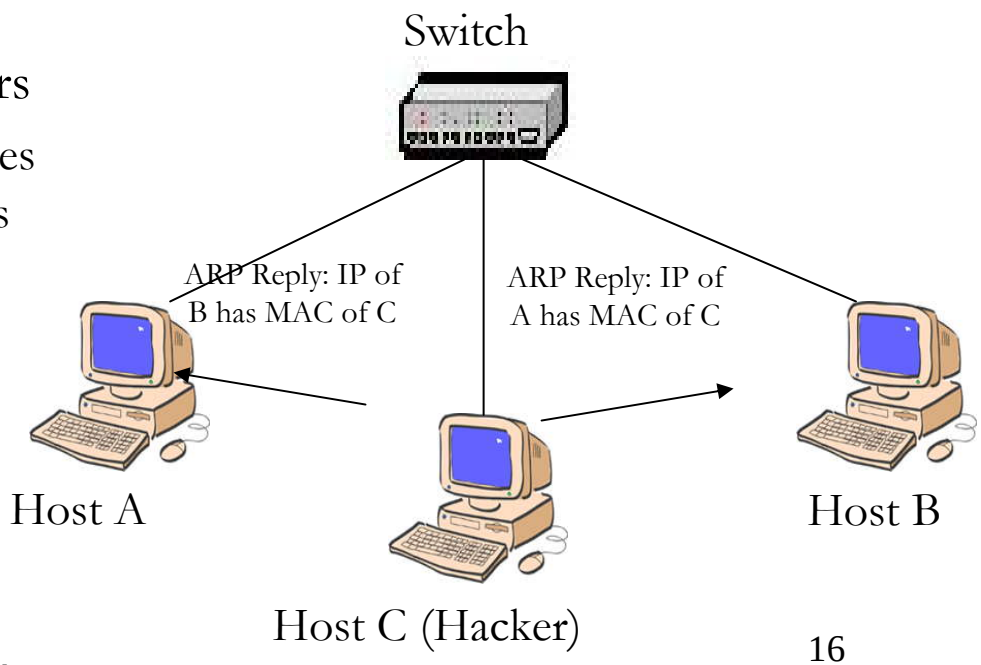
    (e.g. animated GIF that appears to be unanimated)
  - **Service Request Attack:** Increases power consumption by engaging device in servicing invalid network requests.

    (e.g. repeatedly making network requests like telnet, ssh, or web requests to device under attack and draining battery power)

Wireless Insecurity

Eavesdropping: ARP Poisoning

- The Address Resolution Protocol determines the mapping between IP addresses and MAC addresses on local networks.
- ARP caches the values of MAC-to-IP mappings
  - Whenever an ARP request or reply is received the cache is updated
- Hacker sends fake ARP replies to other machines on the network
- The ARP cache poisoning attack can be used against all machines in the same broadcast domain as the attacker.
- ARP poisoning on Wireless routers
  - Attacker obtains packets and frames from the air by "poisoning" caches of MAC/IP combinations of two hosts connected to the "physical" network.



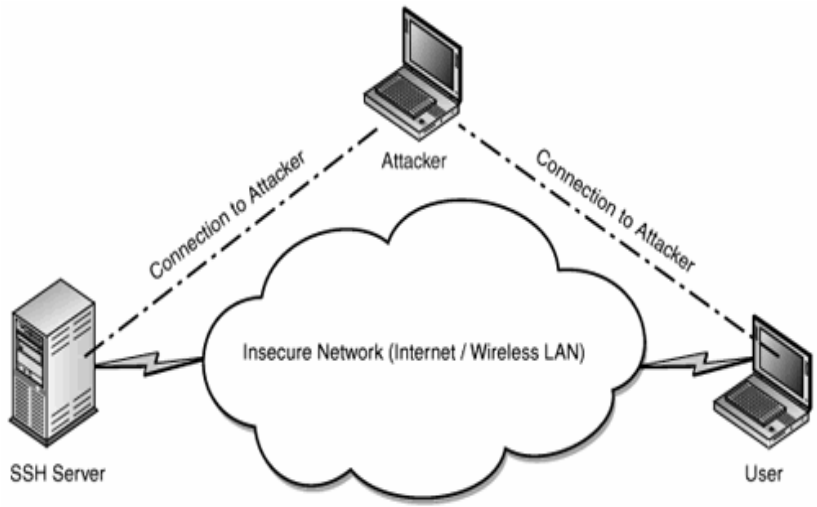
Wireless Insecurity

Eavesdropping: Man in the Middle

Steps:

1. The victim initiates a connection
2. The attacker intercepts the connection and complete the connection to the intended resource
3. The attacker proxies all communication to the resource.
4. Once connected he can modify, eavesdrop, and inject data on the hijacked session

- Used to eavesdrop and manipulate communication



MITM ATTACK
SOURCE: MAXIM, POLLINO: WIRELESS SECURITY 2002

Wireless

Protection – Basic

- Change default administrative passwords
- Turn on Compatible Encryption
- Change the default SSID
- Enable MAC Address Filtering
- Disable SSID broadcast
- Assign static IP addresses to devices
- Position the Router or Access Point Safely

Source: http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

Wireless Security

Service Set Identifier (SSID)

- A mechanism that can segment a wireless network into multiple networks serviced by different APs
  - Each AP is programmed with an SSID that corresponds to a wireless segment
  - To gain access to the network the client must be configured with the appropriate SSID
  - A computer may have multiple SSIDs
- Client computer presents an SSID to the AP
- If broadcast feature is enabled on AP then it is easy to obtain SSID
  - A large fraction of APs do not have an SSID

Wireless Security

MAC Filtering

- Each client computer has a unique MAC address
- An AP can be programmed with a list of MAC addresses that are allowed to connect through it
- Suitable for small networks where MAC addresses can be efficiently managed

Wireless Security

Summary

- Wireless poses severe security vulnerability to networks
- Standard tools are available for hacking into wireless networks
- Risk analysis must incorporate wireless security
- Controls for wireless security only partially effective
  - New controls being developed to address these issues