Wireless Security

Chapter 12

Introduction to Wireless Networking

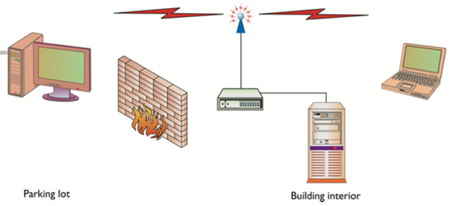
- Wireless networking
  - The transmission of packetized data by means of a physical topology that does not use direct physical links.
- IEEE 802.11 –
  - A family of protocols that have been standardized by the IEEE for wireless local area networks (LANs).
- Wireless Application Protocol (WAP) –
  - One of the pioneers of mobile data applications.
- Bluetooth
  - A short-range wireless protocol typically used on small devices such as mobile phones.

Introduction to Wireless Networking

- The security world ignored wireless for a long time
- Within the space of a few months, it seemed like everyone was attempting to breach the security of wireless networks and transmissions.

- Reasons:
  - One reason wireless suddenly found itself to be such a target is that wireless networks are so abundant and so unsecured.
  - Wireless is particularly problematic from a security standpoint, because there is no control over the physical layer of the traffic.

Wireless Transmission



- Wired LAN
  - The administrators have physical control over the network and can possibly control to some degree who can actually connect to the network
  - Makes snooping around and listening to the traffic difficult.

- Wireless LAN
  - Does away with physical limitations
  - If an attacker can get close to the signal source, it can very least listen to the access point and clients talking to capture all the packets for examination
  - Attacker can try to modify the traffic being sent, or try to send their own traffic to disrupt the system
    - Needs strong two-way encryption as it is essentially susceptible to a man-in-the-middle attack

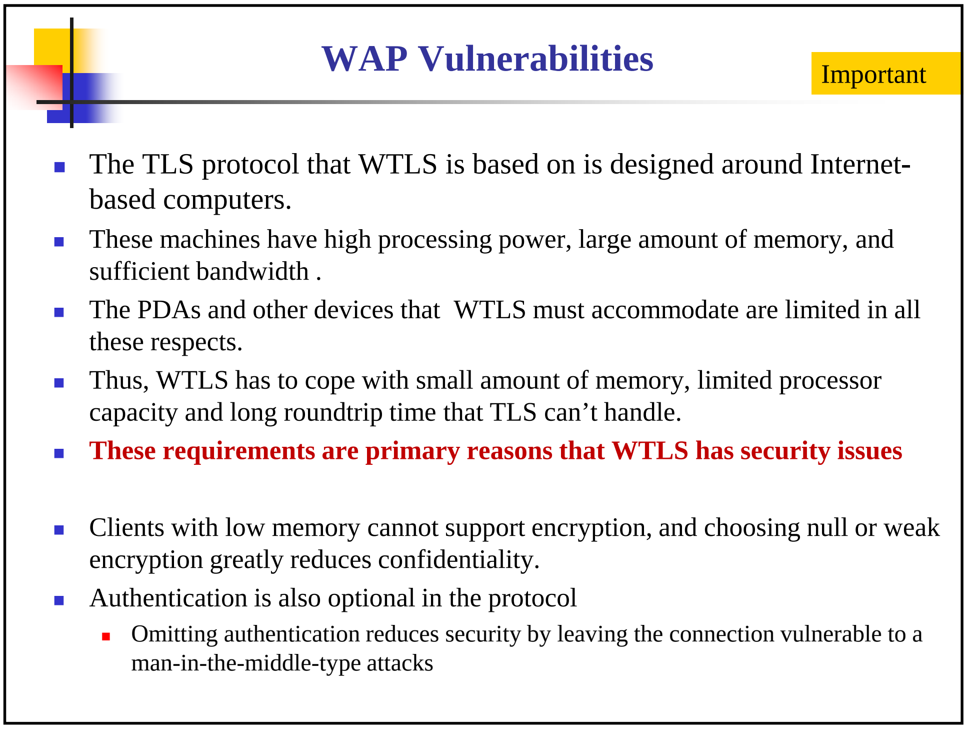
Mobile Phones

- Traditional wireless devices such as cellular phones and pagers are being replaced by wireless e-mail devices and PDAs.
- Almost all current mobile phones have wireless networking features built in.
- Mobile phones have ruthlessly advanced with new technologies and services, causing phones and the carrier networks that support them to be described in generations
  - **1G** refers to the original analog cellular standard, Advanced Mobile Phone System or AMPS.
  - **2G** refers to the digital network that superseded it.
  - **3G** is the system of mobile networks that is currently being deployed.
  - **4G** is planned to run an IP based system utilizing **voice over IP**.

  Features are nice, but what about security??
- Wireless Application Protocol (WAP) attempted to satisfy the needs for more data on mobile devices.

WAP

- Wireless Application Protocol (WAP) is a lightweight protocol designed for mobile devices.
- Wireless Transport Layer Security (WTLS) is a lightweight security protocol designed for WAP.
  - Encrypts the plaintext data and then sends it over the airwaves as ciphertext.
  - Originator and receiver have keys to decrypt the data
- WTLS uses a modified version of the Transport Layer Security (TLS) protocol, formerly known as Secure Sockets Layer (SSL) to **ensure confidentiality.**
- WTLS implements **integrity** through the use of message authentication codes (MACs).
  - A MAC algorithm generates a one-way hash of the compressed WTLS data.

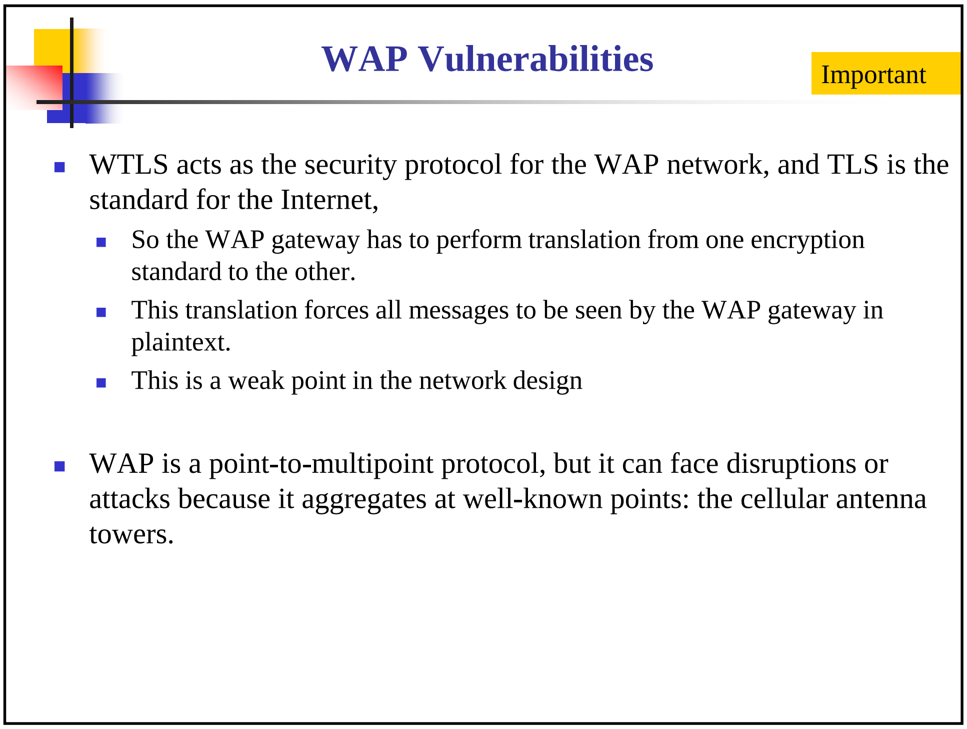


WAP Vulnerabilities

Important

- The TLS protocol that WTLS is based on is designed around Internet-based computers.
- These machines have high processing power, large amount of memory, and sufficient bandwidth .
- The PDAs and other devices that WTLS must accommodate are limited in all these respects.
- Thus, WTLS has to cope with small amount of memory, limited processor capacity and long roundtrip time that TLS can’t handle.
- **These requirements are primary reasons that WTLS has security issues**

- Clients with low memory cannot support encryption, and choosing null or weak encryption greatly reduces confidentiality.
- Authentication is also optional in the protocol
  - Omitting authentication reduces security by leaving the connection vulnerable to a man-in-the-middle-type attacks



WAP Vulnerabilities

Important

- WTLS acts as the security protocol for the WAP network, and TLS is the standard for the Internet,
  - So the WAP gateway has to perform translation from one encryption standard to the other.
  - This translation forces all messages to be seen by the WAP gateway in plaintext.
  - This is a weak point in the network design

- WAP is a point-to-multipoint protocol, but it can face disruptions or attacks because it aggregates at well-known points: the cellular antenna towers.

3G Mobile Networks

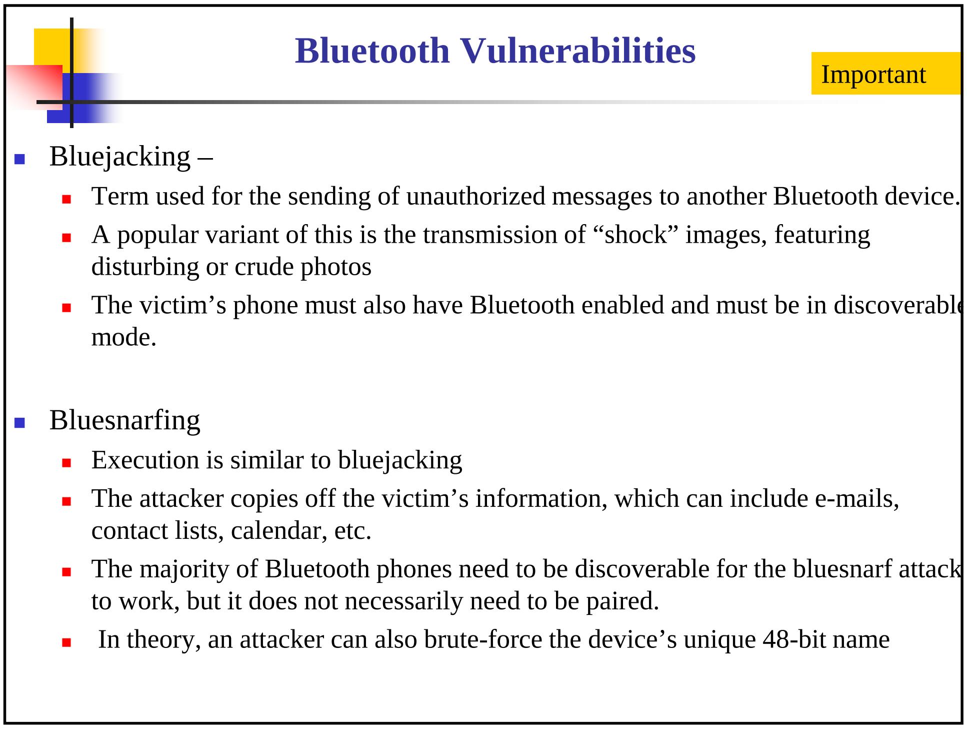
Important

- Mobile wireless networks have been or are being upgraded to 3G, greatly enhancing speed and lowering latency.
- Increased power and memory of handheld devices also reduces the need for lighter-weight encryption protocols.
  - This has caused the protocols used for 3G mobile devices to build in their own encryption protocols.
- The cryptographic standard proposed for 3G is known as KASUMI.
  - Multiple attacks have been launched against these ciphers

Bluetooth

Important

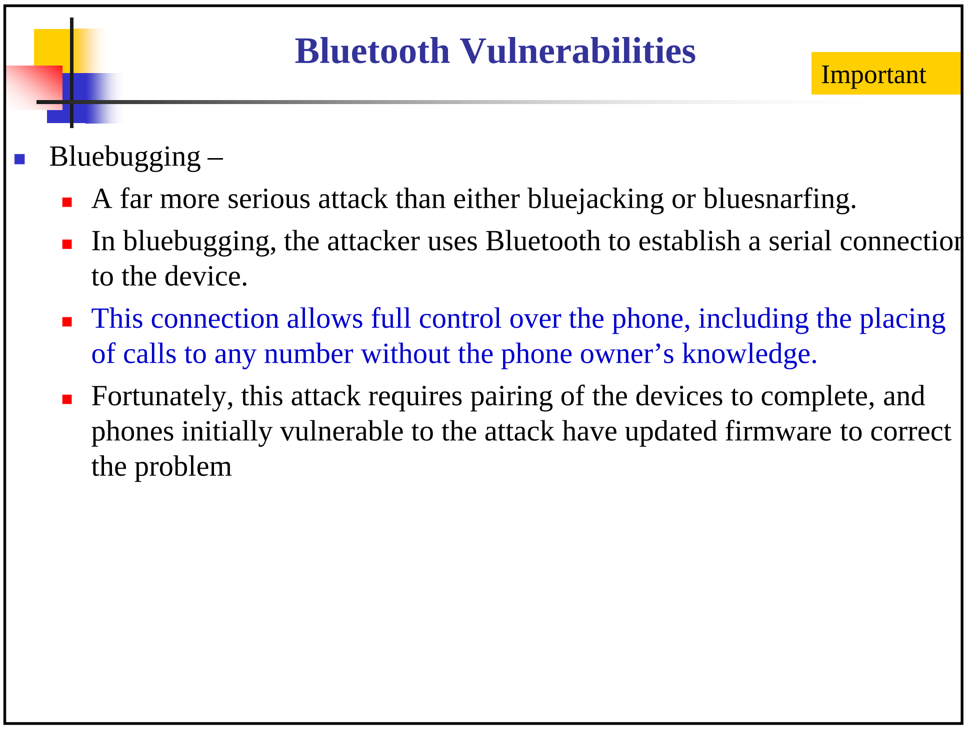
- Bluetooth is a short-range (approx. 32 feet), low-power wireless protocol transmitting in the 2.4 GHz band.
- Bluetooth transmits data in Personal Area Networks (PANs) through mobile phones, laptops, printers, and audio devices.
- As these become popular, people started trying to find holes in it.
- Security issues:
  - Bluetooth features easy configuration of devices to allow communication with no need for network addresses or ports.
  - It uses pairing to establish trust relationship between devices
  - To establish that trust, the devices need advertise capabilities & require passkey
    - To help maintain security, most devices require the passkey to be entered into both devices- this prevents a default passkey – type attack
  - The Bluetooth's protocol advertisement of services and pairing properties is where the security issues start



Bluetooth Vulnerabilities

Important

- Bluejacking –
  - Term used for the sending of unauthorized messages to another Bluetooth device.
  - A popular variant of this is the transmission of “shock” images, featuring disturbing or crude photos
  - The victim’s phone must also have Bluetooth enabled and must be in discoverable mode.
- Bluesnarfing
  - Execution is similar to bluejacking
  - The attacker copies off the victim’s information, which can include e-mails, contact lists, calendar, etc.
  - The majority of Bluetooth phones need to be discoverable for the bluesnarf attack to work, but it does not necessarily need to be paired.
  - In theory, an attacker can also brute-force the device’s unique 48-bit name



Bluetooth Vulnerabilities

Important

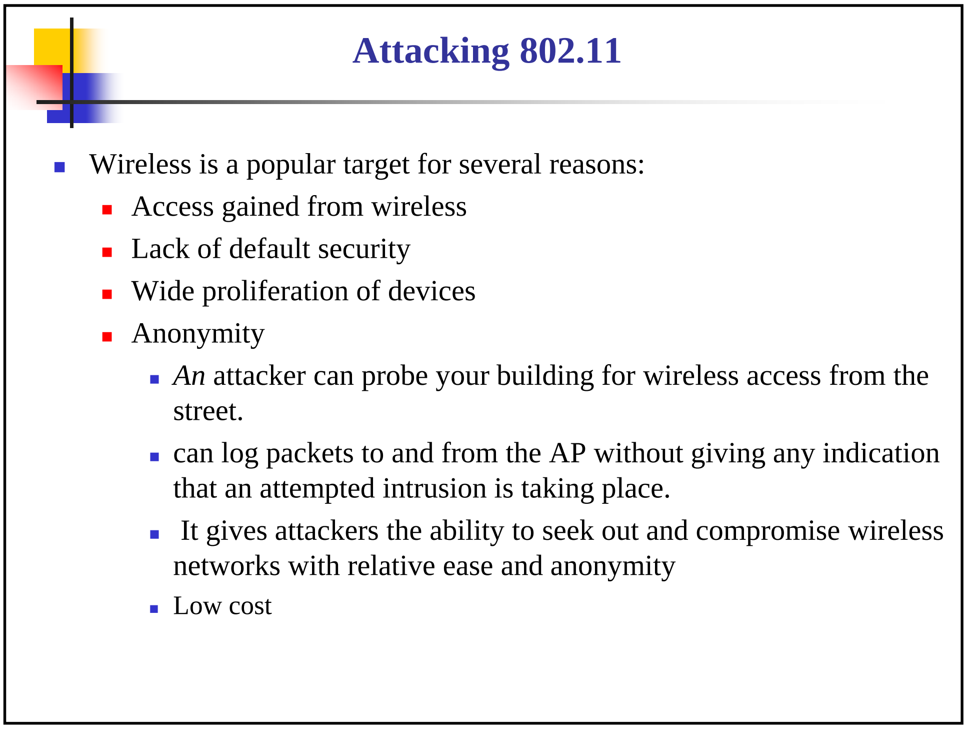
- Bluebugging –
  - A far more serious attack than either bluejacking or bluesnarfing.
  - In bluebugging, the attacker uses Bluetooth to establish a serial connection to the device.
  - This connection allows full control over the phone, including the placing of calls to any number without the phone owner’s knowledge.
  - Fortunately, this attack requires pairing of the devices to complete, and phones initially vulnerable to the attack have updated firmware to correct the problem

802.11

- Group of IEEE standards also called Wi-Fi
- 802.11a
  - wireless networking standard that supports traffic on the 5 GHz band, allowing speeds up to 54 Mbps.
- 802.11b protocol
  - provides for multiple-rate Ethernet over 2.4 GHz spread-spectrum wireless. It provides transfer rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps and uses DSSS.
- 802.11g,
  - Features of 802.11b and 802.11a were joined to create 802.11g,
  - Allows the faster speeds of the 5 GHz specification on the 2.4 GHz band.
- 802.11n
  - on the horizon, with many manufacturers shipping devices based upon the draft specification. 8
  - offers speeds up to 248 Mbps.

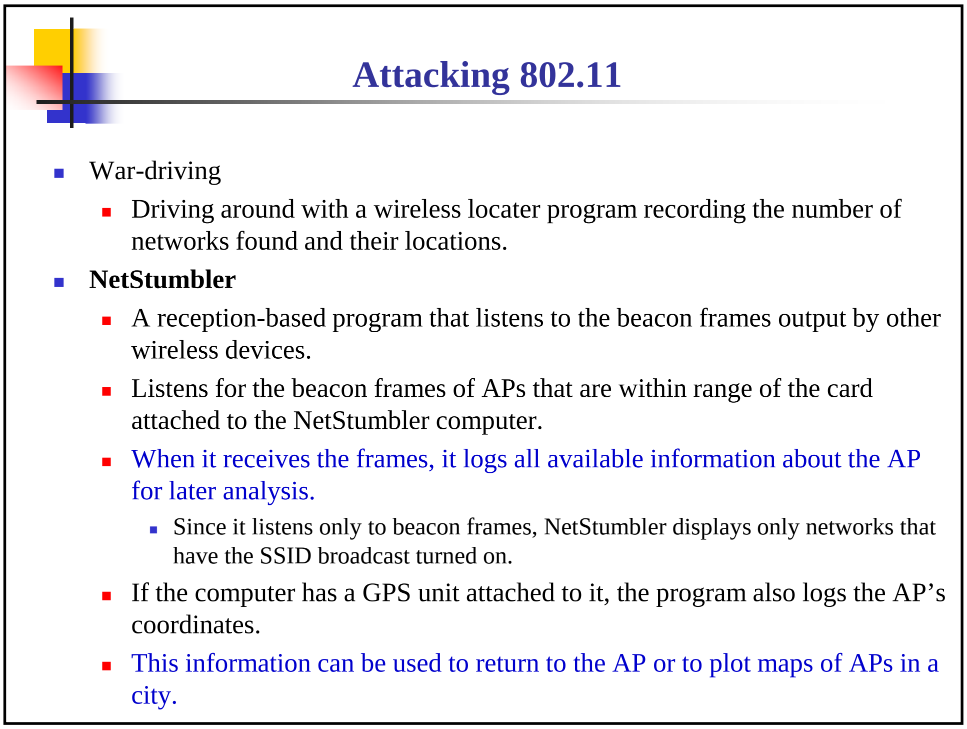
802.11 Protocol

- Authentication
  - Handled in its most basic form by the 802.11 AP, forcing the clients to perform a handshake when attempting to “associate” to the AP.
- Service set identifier (SSID)
  - The SSID is a phrase based authentication mechanism that helps ensure that you are connecting to the correct AP.
  - The SSID setting should limit access only to the authorized users of the wireless network.
  - SSID phrase is transmitted in all the access point’s beacon frames
- Beacon Frame
  - An 802.11 management frame for the network and contains all the information about the network., such as SSID, timestamp
  - Transmitted periodically to announce the presence of a Wireless LAN network
- The designers of 802.11 standard attempted to maintain confidentiality by introducing Wired Equivalent Privacy (WEP)
  - WEP uses the RC4 stream cipher to encrypt the data as it is transmitted through the air.
  - Have an implementation problem that can be exploited to break security



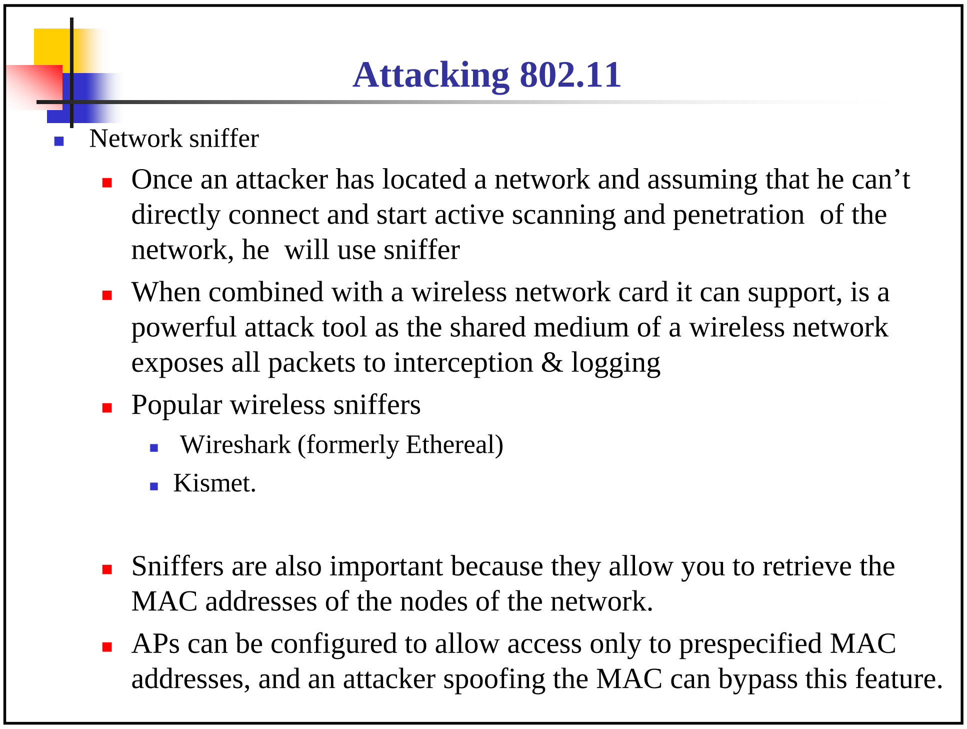
Attacking 802.11

- Wireless is a popular target for several reasons:
  - Access gained from wireless
  - Lack of default security
  - Wide proliferation of devices
  - Anonymity
    - *An* attacker can probe your building for wireless access from the street.
    - can log packets to and from the AP without giving any indication that an attempted intrusion is taking place.
    - It gives attackers the ability to seek out and compromise wireless networks with relative ease and anonymity
    - Low cost



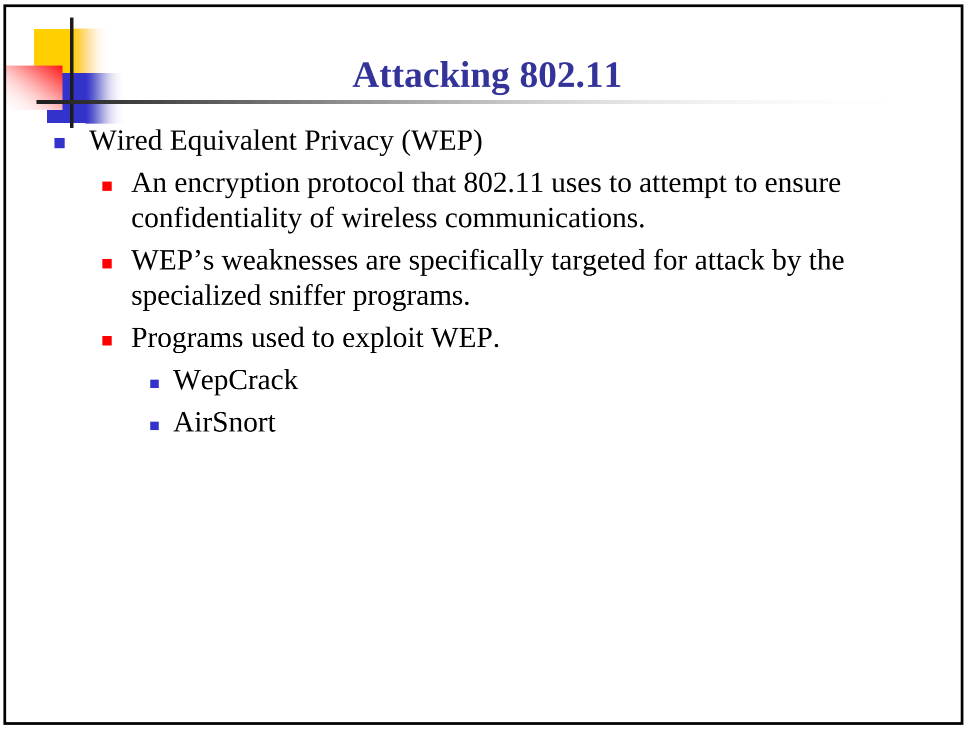
Attacking 802.11

- War-driving
  - Driving around with a wireless locater program recording the number of networks found and their locations.
- **NetStumbler**
  - A reception-based program that listens to the beacon frames output by other wireless devices.
  - Listens for the beacon frames of APs that are within range of the card attached to the NetStumbler computer.
  - When it receives the frames, it logs all available information about the AP for later analysis.
    - Since it listens only to beacon frames, NetStumbler displays only networks that have the SSID broadcast turned on.
  - If the computer has a GPS unit attached to it, the program also logs the AP’s coordinates.
  - This information can be used to return to the AP or to plot maps of APs in a city.



Attacking 802.11

- Network sniffer
  - Once an attacker has located a network and assuming that he can't directly connect and start active scanning and penetration of the network, he will use sniffer
  - When combined with a wireless network card it can support, is a powerful attack tool as the shared medium of a wireless network exposes all packets to interception & logging
  - Popular wireless sniffers
    - Wireshark (formerly Ethereal)
    - Kismet.
  - Sniffers are also important because they allow you to retrieve the MAC addresses of the nodes of the network.
  - APs can be configured to allow access only to prespecified MAC addresses, and an attacker spoofing the MAC can bypass this feature.



Attacking 802.11

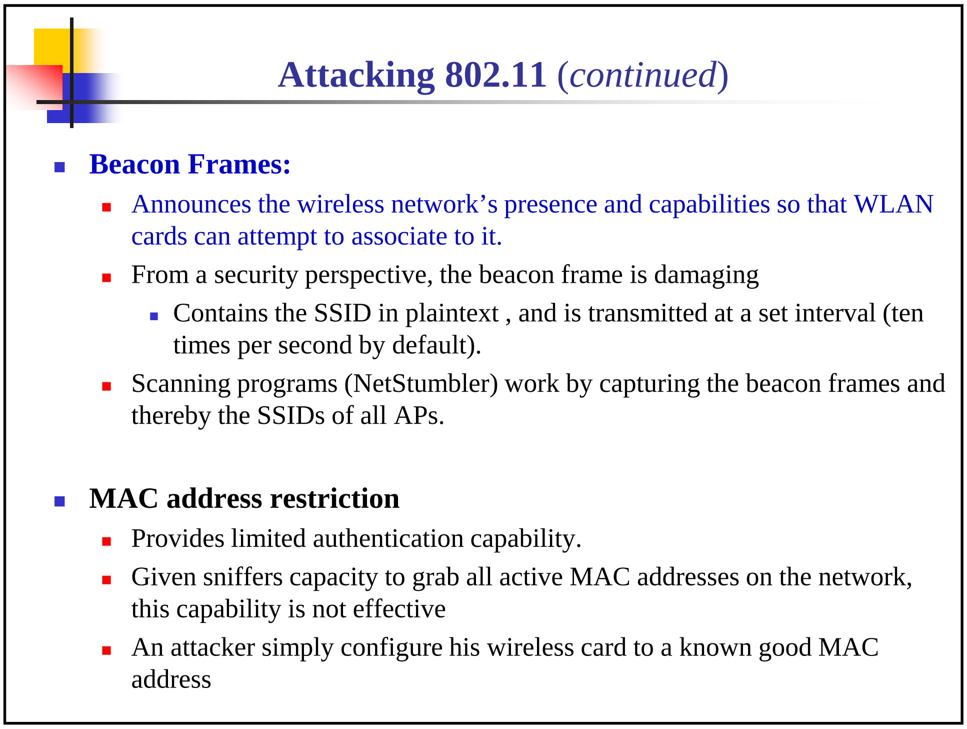
- Wired Equivalent Privacy (WEP)
  - An encryption protocol that 802.11 uses to attempt to ensure confidentiality of wireless communications.
  - WEP's weaknesses are specifically targeted for attack by the specialized sniffer programs.
  - Programs used to exploit WEP.
    - WepCrack
    - AirSnort

Attacking 802.11

- Site survey
  - An important step in securing a wireless network to avoid sending critical data beyond company walls.
  - If anyone attaches a rouge access point to your network, you want to know about it immediately
- A rogue access point
  - An unauthorized wireless access point within an organization.
  - Can be set up by well-meaning employees or hidden by an attacker with physical access.
    - Also by sneaking into the building briefly.
  - The attacker can set up an AP on the network and, by placing it behind the external firewall or network IDS (NIDS) type of security measures, can attach to the wireless at a later date at their leisure.

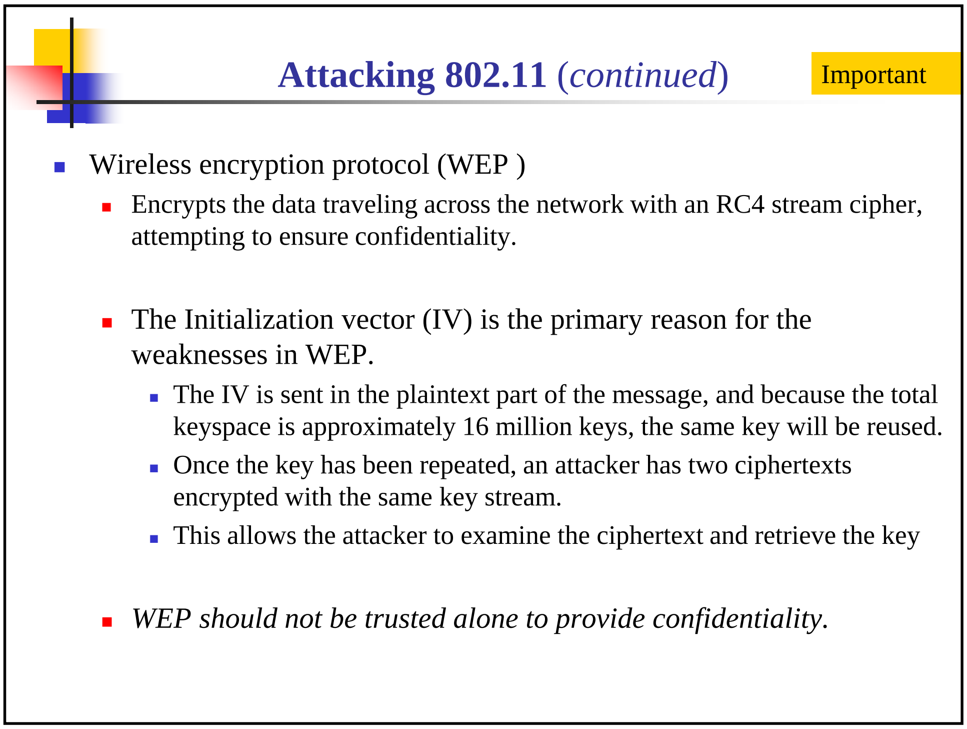
Attacking 802.11 (*continued*)

- Service set identifier (SSID)
  - Unique 32-character attached to the header of the packet
  - Many APs also use a default SSID-
    - for Cisco APs, this default is *tsunami*, which may indicate an AP that has not been configured for any security.
  - Renaming the SSID and disabling SSID broadcast are necessary
    - However, because the SSID is part of every frame, these measures should not be considered adequate to secure the network.
  - Any sniffer can determine the SSID
    - While the SSID is a good idea in theory, it is sent in plaintext in the packets
    - So in practice, SSID offers little security significance
  - Operating systems display a list of SSIDs active in the area and prompt the user to choose which one to connect to



Attacking 802.11 *(continued)*

- **Beacon Frames:**
  - Announces the wireless network’s presence and capabilities so that WLAN cards can attempt to associate to it.
  - From a security perspective, the beacon frame is damaging
    - Contains the SSID in plaintext , and is transmitted at a set interval (ten times per second by default).
  - Scanning programs (NetStumbler) work by capturing the beacon frames and thereby the SSIDs of all APs.
- **MAC address restriction**
  - Provides limited authentication capability.
  - Given sniffers capacity to grab all active MAC addresses on the network, this capability is not effective
  - An attacker simply configure his wireless card to a known good MAC address



Attacking 802.11 *(continued)*

Important

- Wireless encryption protocol (WEP)
  - Encrypts the data traveling across the network with an RC4 stream cipher, attempting to ensure confidentiality.
  - The Initialization vector (IV) is the primary reason for the weaknesses in WEP.
    - The IV is sent in the plaintext part of the message, and because the total keyspace is approximately 16 million keys, the same key will be reused.
    - Once the key has been repeated, an attacker has two ciphertexts encrypted with the same key stream.
    - This allows the attacker to examine the ciphertext and retrieve the key
  - *WEP should not be trusted alone to provide confidentiality.*