Wireless Based Attacks

Objectives

- Explain how wireless networks work
- Discuss threats against wireless networks
- Understand how to protect yourself when on an untrusted wireless network

Wireless is everywhere!

- Some organizations don’t even put wired ports in anymore
- Nearly all devices out there come with some kind of wireless connection
- We get frustrated if we don’t have signal

How wireless works

- What do we need to know?
  - Channels – 20Ghz, 40Ghz, 80Ghz
    - Lower the frequency, lower the speed
  - Base station serves an SSID
  - Client connects to an SSID (Service Set Identifier)
  - SSID can be really most anything!

Threats to clients

- Connecting to a spoofed SSID
  - Attacker/owner can sniff traffic
- Connecting to unsecured SSID (open)
  - Attacker could perform a man in the middle attack
- Denial of service – sending disconnects

Threats to infrastructure

- Signal interference – too many APs or SSIDs
- Spoofing SSIDs
- WPS – Wifi protected setup
- Usernames/passwords
- Backdoors
- What was protected through wires, now allows anyone to connect

Threats to communications

- SSID is secured with WEP (Wireless Equivalent Privacy)
  - Keys can be obtained within seconds
- Untrusted networks
- Encryption is not built into Open SSIDs

Defenses

- Use trusted networks
- Secure SSIDs using well known and secure protocols
- Only broadcast where you intent to use the signal (physicality)